<<
Data Prot ssment

Company Name:		nt Downloaded:	
Registered Address:		act:	
Premises Address:		Carried Out By:	
Description:		Date (or Period):	
Project:			

Part 1: Business and Project Summary

Question Ref.	Question	Answer		Answer Date
1.1	What are the business's aims and objectives?			
1.2	Provide a brief summary of the project.			
1.3	What are the aims and objectives of the project?			
1.4	What are the intended and expected outcomes of the project for data subjects?			
1.5	Which codes of conduct, codes of practice, and/or certification schemes apply to the project?			

Part 2: Is a Data Protection Impact Assessment

Question Ref.	Question	Answer		Answer Date
2.1	Will the project involve the collection, storage, and/or use of personal data?			
2.2	Will the personal data used in the project be: a) Newly-collected data; or b) Existing data used for a new purpose or in a new way?			
2.3	Will the personal data collected be obtained: a) From data subjects directly; or b) From other sources?			
2.3.1	If personal data is to be obtained from other sources, will this be done without providing the individual with a privacy notice? ('invisible processing')			
2.4	List the type(s) of personal data that will be used in the project.			
2.4.1	If any of the personal data listed above is special category personal data, note that here, providing a brief description of how it will be used.			
2.4.2	If any of the personal data listed above is biometric or genetic data, note that here, providing a brief description of how it will be used.			
2.4.3	Is special category personal data (or criminal offence data) being processed on a large scale? If yes,			

Question Ref.	Question	Answer		Answer Date
	provide a brief description.			
2.4.4	Is special category personal data to be used to decide on individuals' access to services? If yes, provide a brief description.			
2.4.5	Will any personal data (and/or special category personal data) concerning children or other vulnerable individuals be processed? If yes, provide a brief description.			
2.5	Will the project utilise novel types of personal data processing?			
2.5.1	If yes, provide a brief description of the processing.			
2.6	Will the project utilise new technology that may be considered high-risk or otherwise intrusive to privacy?			
2.6.1	If yes, provide a brief description of the technology.			
2.7	Will the project use personal data for automated decision-making or profiling?			
2.7.1	If yes, provide a brief description.			
2.7.2	Will profiling be used to decide on individuals' access to services? If yes, provide a brief description.			
2.8	Will individuals be profiled on a large scale?			

Question Ref.	Question	Answer			Answer Date
2.8.1	If yes, provide a brief description.				
2.9	Will the project involve the systematic monitoring of publicly accessible places on a large scale?				
2.9.1	If yes, provide a brief description.				
2.10	Will the project involve the matching or combination of datasets from different sources?				
2.10.1	If yes, provide a brief description.				
2.11	Will the project involve tracking individuals' location or behaviour?				
2.11.1	If yes, provide a brief description.				
2.12	Will the project involve profiling children or targeting services to them?				
2.12.1	If yes, provide a brief description.				
2.13	Will the project involve processing personal data that may endanger individuals' physical health or safety in the event of a security breach?				
2.13.1	If yes, provide a brief description.				
2.14	Will the project involve systematic and extensive profiling with significant effects?				
2.14.1	If yes, provide a brief description.				

Question Ref.	Question	Answer		Answer Date
2.15	Will the project involve the sharing of personal data with third parties?			
2.15.1	If yes, list those third parties, including their location.			
2.16	Does the project relate to any current issues of public concern?			
2.16.1	If yes, state how the project relates and whether those issues relate positively or negatively to the project.			
Is a Data Protection Impact Assessment Required?				
2.17	In light of the answers provided above in Part 2, is a Data Protection Impact Assessment required?			
2.17.1	Provide an outline of the reason(s) for the answer to 2.17.			

Part 3: Consultation

Question Ref.	Name	Contact Details	When the Party will be Consulted	Answer Date
Provide details of the internal parties to be consulted for this Data			**ssment (add or remove rows as required):**	
3.1				
3.2				
3.3				
3.4				
3.5				
3.6				
3.7				
3.8				
3.9				
3.10				
Provide details of the external parties to be consulted for this Dat			**ssment (add or remove rows as required):**	
3.11				
3.12				
3.13				
3.14				
3.15				
3.16				

Part 4: Data Subjects, Personal Data, Collectio e

Question Ref.	Question	Answer		Answer Date
4.1	Refer back to 2.4 and list the personal data that will be used in the project here (list special category personal data, where applicable, separately).			
For each item under 4.1, answer the following:				
4.2	How will the personal data be collected?			
4.3	What volume of personal data will be collected?			
4.4	How many data subjects will be involved?			
4.5	What geographical area will the project cover?			
4.6	What categories of data subject will be involved?			
4.7	What is, or will be, the nature of the business's relationship with the data subjects involved?			
4.8	How will the personal data be used?			
4.9	What will be the extent and frequency of the personal data processing?			
4.10	Does the business have prior experience with this type of personal data processing?			

Question Ref.	Question	Answer			Answer Date
4.11	To what extent are individuals likely to expect the proposed processing?				
4.12	How will the personal data be stored?				
4.13	Where will the personal data be stored?				
4.14	Who will have access to the personal data and for what purpose(s)?				
4.15	Will the personal data be shared and for what purpose(s)?				
4.16	Will third-party data processors be used and for what purpose(s)?				
4.17	What lawful basis (or bases) for processing the personal data is or are being relied upon?				
4.18	How long will the processing of the personal data continue (or, if this is not known, how will the duration be determined)?				
4.19	How long will the personal data be held (or, if this is not known, how will the length of its retention be determined)?				
4.20	When the retention period has expired, the personal data is no longer required, or is otherwise to be deleted or disposed of, how will this be done?				
4.21	What controls will individual data				

Question Ref.	Question	Answer		Answer Date
	subjects be given over their personal data?			
4.22	What organisational security measures are proposed to protect the personal data?			
4.23	What technical security measures are proposed to protect the personal data?			
4.24	Have there been any advances in technology or security that could be applied to the project?			

Part 5: Impact on Data Subjects

Question Ref.	Potential Risk	Severity of Imp	Notes / Comments	Answer Date
5.1	Personal data being used in a manner not covered by the lawful basis or bases identified under 4.17.	low/medium/hig		
5.2	Data subjects not being made fully (and clearly) aware of the purpose(s) for which their personal data is used.	low/medium/hig		
5.3	Collecting more personal data than data subjects are informed about.	low/medium/hig		
5.4	Collecting more personal data than is reasonably necessary for the purpose(s) for which it is to be used.	low/medium/hig		
5.5	Collecting personal data about vulnerable people and not sufficiently addressing their concerns about that collection.	low/medium/hig		
5.6	Collecting special category ('sensitive') personal data.	low/medium/hig		
5.7	Data subjects not being made aware of the lawful basis or bases identified under 4.17.	low/medium/hig		
5.8	Data subjects not being given the information required by Articles 13 and/or 14 of the UK GDPR (including that under 5.2, 5.7, 5.9, and information about their rights under the UK GDPR).	low/medium/hig		
5.9	Personal data being shared with third parties without data subjects'	low/medium/hig		

Question Ref.	Potential Risk	Severity of Imp	Notes / Comments	Answer Date
	knowledge and/or consent.			
5.10	Personal data being revealed to third parties accidentally as a result of insufficient controls on disclosure.	low/medium/hig		
5.11	The use of personal data extending beyond the purpose(s) for which it is initially collected without data subjects' knowledge and/or consent (where consent is required).	low/medium/hig		
5.12	Anonymity being compromised where the combination of data sets results in anonymous identifiers or pseudonymised data becoming data that is capable of identifying individual data subjects.	low/medium/hig		
5.13	Personal data not being checked for accuracy at or after collection.	low/medium/hig		
5.14	Personal data not being kept up-to-date.	low/medium/hig		
5.15	Personal data being retained for longer than is necessary in light of the purpose(s) for which it is collected.	low/medium/hig		
5.16	Personal data being used in a manner that is not permitted by the data subject (e.g. where a data subject has exercised the right to restrict processing).	low/medium/hig		
5.17	Data subjects' exercise of their rights under the UK GDPR (including but not limited to the rights of access,	low/medium/hig		

Question Ref.	Potential Risk	Severity of		Notes / Comments	Answer Date
	rectification, erasure, restricting processing, objecting to processing, and data portability) being impeded.				
	<<Add further risks as required>>	low/medium			

Part 6: Organisational Risks

Question Ref.	Potential Risk	Severity of Imp	lotes / Comments	Answer Date
6.1	Non-compliance with the UK GDPR or other data protection and privacy-related legislation resulting in damage to reputation.	low/medium/hig		
6.2	Further risks or issues being identified at a later stage in the project (after this assessment) or once the project has been implemented, requiring costly remedial action rather than building in preventative measures.	low/medium/hig		
6.3	The use of personal data in a way that causes concern among data subjects resulting in reluctance to deal with the business and/or damage to reputation.	low/medium/hig		
6.4	Insufficient transparency surrounding personal data use resulting in reluctance to deal with the business and/or damage to reputation.	low/medium/hig		
6.5	Excessive or unnecessary storage of personal data which, in addition to the risks identified under 5.3 and 5.4, may result in the data being less useful and compromising efficiency.	low/medium/hig		
6.6	Poor perception by data subjects about the business's use of personal data resulting in damage to reputation.	low/medium/hig		
	<<Add further risks as required>>	low/medium/hig		

Part 7: Compliance and Legal Risks

Question Ref.	Potential Risk	Severity of Imp	Notes / Comments	Answer Date
7.1	Non-compliance with the UK GDPR or other data protection and privacy-related legislation resulting in fines and other possible penalties.	low/medium/hig		
7.2	Non-compliance with the Privacy and Electronic Communications Regulations (PECR).	low/medium/hig		
7.3	Non-compliance with other relevant legislation.	low/medium/hig		
	<<Add further risks as required>>	low/medium/hig		

Part 8: Solutions to Identified Risks

Question Ref.	Potential Solution	Potential Risk(s) Add (Question Ref.)		Evaluation of Solution	Answer Date
Evaluate the following with respect to the Impact on Data Subject			**ether the risk is likely to be eliminated entirely, reduced (and to what degree), or accepted. Under *Evaluation,* state whether the fi**	**ng into account the potential solution, is justifiable and what its final impact will be on the project from a cost/benefit perspecti**	
8.1	Controlling the use of personal data, limiting use to that compatible with the lawful basis or bases established under 4.17 and with the purpose(s) for which the data is originally collected.	5.1, 5.11			
8.2	If additional use(s) of personal data is necessary, inform data subjects and, where required, obtain their consent to the additional use(s).	5.11			
8.3	Collecting only the personal data that is reasonably required for the stated purpose(s).	5.3, 5.4			
8.4	Provide clear information about the business's use of personal data to data subjects including what is collected, for what purpose(s), on what legal basis etc.	5.2, 5.3, 5.7, 5.8			
8.5	Provide other important information required under Articles 13 and 14 of the UK GDPR in a clear, concise, and accessible manner.	5.8			

Question Ref.	Potential Solution	Potential Risk(s) Add (Question Ref.)		Evaluation of Solution	Answer Date
8.6	Only collect, process, and store special category personal data where absolutely necessary. Question whether it is required for the stated purpose(s). Ensure that one of the conditions under UK data protection legislation is met.	5.6			
8.7	Ensure that all data subjects, and particularly those that are vulnerable, can easily find answers to their questions about the business's use of their personal data.	5.2, 5.5			
8.8	Control all personal data sharing with third parties. Choose trustworthy, reputable data processors. Ensure that all sharing is documented and made subject to suitable data processing agreements.	5.9, 5.10			
8.9	Inform data subjects of any and all personal data sharing with third parties, obtaining consent where necessary.	5.9, 5.10			
8.10	Where any anonymised or pseudonymised data is used, suitable measures are taken to prevent the identification of individuals, particularly where different data sets are combined.	5.12			

Question Ref.	Potential Solution	Potential Risk(s) Add (Question Ref.)		Evaluation of Solution	Answer Date
8.11	Check all personal data for accuracy, where reasonably possible, at the time of collection and at regular intervals thereafter. Provide easy, accessible means for data subjects to update their own personal data held by the business.	5.13, 5.14			
8.12	Establish data retention periods prior to the collection of personal data or, where a fixed period cannot be reasonably established, determine criteria upon which the retention of personal data will be decided. Review regularly.	5.15			
8.13	Implement (or update, as appropriate) the business's Data Retention Policy.	5.15			
8.14	Ensure the secure destruction (or disposal) of personal data that is no longer to be retained.	5.15			
8.15	Ensure that data subjects are given information about their rights under Chapter 3 of the UK GDPR and how to exercise them.	5.16, 5.17			
8.16	Cooperate fully with any and all requests by data subjects to exercise their rights under Chapter 3 of the UK GDPR and provide easy and accessible	5.16, 5.17			

Question Ref.	Potential Solution	Potential Risk(s) Add (Question Ref.)		Evaluation of Solution	Answer Date
	means for them to make such requests.				
Evaluate the following with respect to Organisational, Compliance			***Result*, state whether the risk is likely to be eliminated entirely, reduced (and to what degree), or accepted. Under *Evalua***	**nal impact of the risk, taking into account the potential solution, is justifiable and what its final impact will be on the proj**	**rspective.**
8.17	Ensure that the business's Data Protection Policy is followed at all times (and updated if necessary to factor in the project).	6.1, 7.1, 7.2, 7.3			
8.18	Ensure that all staff associated with the project are fully trained in all related aspects of data-protection (including but not limited to the legal requirements of the UK GDPR and other applicable data protection and privacy legislation) and are made aware of all potential risks.	6.1, 7.1, 7.2, 7.3			
8.19	Implement suitable organisational security measures to protect personal data.	6.1, 7.1, 7.2, 7.3			
8.20	Implement suitable technical security measures to protect personal data.	6.1, 7.1, 7.2, 7.3			
8.21	Address data protection risks thoroughly at this part of the planning stage of the project and implement agreed	6.2			

Question Ref.	Potential Solution	Potential Risk(s) Addr (Question Ref.)		Evaluation of Solution	Answer Date
	solutions as the project progresses, reviewing at regular intervals wherenecessary.				
8.22	Controlling the use of personal data, limiting use to that compatible with the lawful basis or bases established under 4.7 and with the purpose(s) for which the data is originally collected. (See 8.1)	6.3, 6.6			
8.23	Only collect, process, and store special category personal data where absolutely necessary. Question whether it is required for the stated purpose(s). Ensure that one of the conditions under UK data protection legislation is met. (See 8.6)	6.3, 6.6			
8.24	Provide clear information about the business's use of personal data to data subjects including what is collected, for what purpose(s), on what legal basis etc. (See 8.4)	6.3, 6.4, 6.6			
8.25	Ensure that all data subjects, and particularly those that are vulnerable, can easily find answers to their questions about the business's use of their personal data. (See 8.7)	6.3, 6.4, 6.6			

Question Ref.	Potential Solution	Potential Risk(s) Add (Question Ref.)		Evaluation of Solution	Answer Date
8.26	Ensure that data subjects are given information about their rights under the Chapter 3 of the UK GDPR and how to exercise them. (See 8.15)	6.3, 6,4 6.6			
8.27	Cooperate fully with any and all requests by data subjects to exercise their rights under the Chapter 3 of the UK GDPR and provide easy and accessible means for them to make such requests. (See 8.16)	6.3, 6.4, 6.6			
8.28	Collecting only the personal data that is reasonably required for the stated purpose(s). (See 8.3)	6.5			
8.29	Establish data retention periods prior to the collection of personal data or, where a fixed period cannot be reasonably established, determine criteria upon which the retention of personal data will be decided. Review regularly. (See 8.12)	6.5			
8.30	Implement (or update, as appropriate) the business's Data Retention Policy. (see 8.13)	6.5			
8.31	Ensure the secure destruction (or disposal) of personal data that is no longer to be retained. (See 8.14)	6.5			

Question Ref.	Potential Solution	Potential Risk(s) Add (Question Ref.)		Evaluation of Solution	Answer Date
	<<Add further solutions as required>>				

Part 9: Approved Solutions

Risk (Include Question Ref.)	Approved Solution (Include Question Ref.)		Notes / Comments	Approval Date
<<Add further risks as required>>	<<Add further solutions as required>>			

Part 10: Integration of Data Protection Impact A mes into Project Plan

Action to be Taken	Completion Date (or Fr	ty for Action	Notes / Comments
Integrate the outcomes of this Data Protection Impact Assessment into the main project plan, updating additional project documentation as necessary.		e>>	
Implement approved privacy risk solutions.		e>>	
Review this Data Protection Impact Assessment and the project plan regularly.		e>>	
Update this Data Protection Impact Assessment and the project plan as required.		e>>	
Conduct internal and external consultations as required.		e>>	
<<describe specific actions to be taken based on approved solutions>>		e>>	
<<describe specific actions to be taken based on approved solutions>>		e>>	
<<describe specific actions to be taken based on approved solutions>>		e>>	
<<describe specific actions to be taken based on approved solutions>>		e>>	
<<describe specific actions to be taken based on approved solutions>>		e>>	
<<describe specific actions to be taken based on approved solutions>>		e>>	
<<describe specific actions to be taken		e>>	

Action to be Taken	Completion Date (or Fr	y for Action	Notes / Comments
based on approved solutions>>			
<<describe specific actions to be taken based on approved solutions>>		>>	
<<describe specific actions to be taken based on approved solutions>>		>>	
<<describe specific actions to be taken based on approved solutions>>		>>	
<<describe specific actions to be taken based on approved solutions>>		>>	
<<describe specific actions to be taken based on approved solutions>>		>>	
<<describe specific actions to be taken based on approved solutions>>		>>	
<<describe specific actions to be taken based on approved solutions>>		>>	
<<describe specific actions to be taken based on approved solutions>>		>>	
<<describe specific actions to be taken based on approved solutions>>		>>	
<<describe specific actions to be taken based on approved solutions>>		>>	
<<describe specific actions to be taken based on approved solutions>>		>>	
<<Add further actions as required>>		>>	

Part 11: Approval and Sign-Off

[I**] OR [**We**]** hereby confirm that **[**I**] OR [**We**]** have reviewed and ection Impact Assessment. In particular, **[**I am**] OR [**We are**]** satisfied that:

1) The proposed project complies with the core principles s UK GDPR;
2) The proposed collection, processing, and holding of pers one of the conditions set out in Article 6 of the UK GDPR;
3) **[**The proposed collection, processing, and holding of spe ata, in addition to the above, meets at least one of the conditions set out in Article 9 of the UK GDPR;**]**
4) The proposed project and approved solutions complies w jects as set out in Chapter 3 of the UK GDPR;
5) All relevant privacy risks and approved solutions have be ngements have been made to monitor the same at regular intervals throughout the proposed project; and
6) The approved solutions set out herein represent a target portionate response to the privacy risks identified herein.

Name[s]: <<insert name(s)>>
Position[s]: <<insert position(s)>>
Date: <<insert date>>