TEMPLATE – DATA PROTECTION IMPACT ASSESSMENT

To comply with the GDPR, employers are required to conduct a DPIA where there processing of personal data is likely to result in a high risk to the rights and freedoms of data subjects and if that applies, then a DPIA must be undertaken before the processing begins.

In practice, it is unlikely that a training business will be introducing a process which carries such a high risk – however it is possible if, say, an automated process was being introduced for assessing an attendance bonus, with the eligibility being based on the use of an automatic system for clocking in and out.

Even if you do not fall into the legal requirement to conduct a DPIA for a particular process, it can be a useful way of identifying, assessing and address data protection risks and demonstrating that you have done so.

DPIA – Initial stage – Project outline and DPIA screening questions

Consider and set down what the project involves and who the key parties are. Describe the aims of the project, including the benefits to the company, to employees and to any other parties. If there are other documents relating to the project, provide links to those.

Stage 1 – Assess the risk

Assess whether the project involves the processing of personal data which is likely to result in a high risk to individual rights and freedoms and thus whether a DPIA will be necessary.

Question	Yes	No
Will the project involve the collection of new personal data about individuals?		
Will the project compel individuals to provide personal data about themselves?		
Will you be using personal data that you already hold for a purpose it is not currently used for, or in a way it is not currently used?		
Will personal data be disclosed to organisations or people who have not previously had routine access to the information?		
Does the project involve you using new technology which might be perceived as being privacy intrusive e.g. biometrics or facial recognition?		
Is the personal data that will be processed likely to raise privacy concerns or expectations e.g. health data, criminal records data, or other information that people would consider private?		
Will the project result in you evaluating or scoring individuals, making decisions or taking action against them in ways which can have a significant impact on them?		
Does the project involve the systematic monitoring of individuals?		
Will you be processing the personal data of large numbers of individuals?		

If you answer "yes" to two or more of the above questions, this indicates that you should conduct a DPIA in respect of the processing – see next stage.

If you have answered "yes" to fewer than two of the screening question, you must still consider the situation and think about whether the proposed processing is likely to result in a high risk to the rights and freedoms of data subjects, such that you should conduct a DPIA.

You should bear in mind that under data protection law employees are considered to be "vulnerable data subjects" in view of the imbalance of the employer-employee relationship and so you need to be sure that you have good reason(s) for not conducting the DPIA and record the reason(s) in the box below.

Reasons for not conducting a DPIA

Stage 2 - Identify what personal data is to be processed and the purposes of processing?

1. Identify the individuals or the types of individuals to whom the personal data relates
2. List the categories of personal data (e.g. names, dates of birth, CCTV images) and the reason why each category of personal data must be processed for this project
3. Specify whether the project involves the processing of “special category” personal data and if so, what types of special category data and the reason why they must be processed for this project

4. Data Minimisation – are all categories of personal date and special category data listed above really necessary for this project or are there some that you could exclude?
5. Consider the necessity and proportionality of the processing in relation to the purposes described above i.e. is there a practicable way to achieve those proposes that involves processing less personal data?

Stage 3 – Identify the information flow

1 Described the collection, use and deletion of personal data – including any creation, access and sharing that will be involved for each data processing activity in the project. It may be useful to include a flow diagram or other way of explaining data flows. Include information about the volume of data involved and/or the number of individuals likely to be affected by the project.

Stage 4 –Compliance considerations

1. For each category of personal data identified at Stage 1 specify the legal basis for processing. For special category data, you must specify both an ordinary legal basis and a special category legal basis. (See the appendix for a list of ordinary and special category legal bases that are most commonly applicable when processing personal data for employees).
2. It is important that individuals whose personal data will be processed as part of the project are informed as to what is happening with their data. Is this covered by existing privacy notices already provided to the affected individuals or is a new or revised privacy notice needed?
3. Does the project involve the use of existing personal data for new purposes? If yes, is the new purpose compatible with the original purpose for which the personal data was collected?
4. Are you able to amend the personal data where necessary to ensure it is up to date, or ensure that individuals update their own information?

5. What are the retention periods for the personal data and how will these be implemented? i.e. how will data be deleted. If there are different retention periods for different categories of data, then provide details for each period.
6. Are there any exceptional circumstances for retaining certain data for longer than the retention period set out above and how will you identify whether these apply in individual cases?
7. How will you action requests from individuals (or someone acting on their behalf) to exercise their individual rights e.g. Subject Access request, right to be forgotten, objection to processing, etc? Does the project/structure/design enable you to access personal data quickly and easily so that you can respond to such requests in a timely manner and where relevant, within the one month deadline?
8. How will you ensure that all staff with access to the personal data have adequate training on data protection compliance requirements?
9. Will any new or updated policies or procedures be required to implement the project?

10. What security measures are built in to the project structure/design?
11. Will personal data be disclosed internally or externally and, if so, to whom, how and why?
12. If personal data will be disclosed to a third party, are they a data processor? If so, have you put in place an appropriate contract to ensure GDPR compliance?
13. Will personal data be transferred to a country outside the European Economic Area? If so, yes, what arrangements will be put in place to ensure compliance with the GDPR's rules on overseas transfers?

Stage 5 – Consultation

1. Have you sought advice and/or discussed the project with the person who has responsibility for data protection within your organisation? Summarise any advice or discussion?

2. Is there anyone else within the organisation who should be involved in the DPIA (e.g. IT, legal etc)? If so, ensure you integrate their input into your responses across this form, and summarise any additional comments they may have here.
3. The GDPR requires you to consult affected data subjects (or their representatives) about the project "where appropriate"? Have you consulted and, if so, with whom (e.g. individuals data subjects/employee representatives/recognised trade union)? If you have decided not to consult affected data subjects/their representatives about the project, you must document your reasons for this decision.
4. If you have consulted affected data subjects/their representatives, what was their view on this project? If the consultees oppose the project and you plan to go ahead anyway, you must document your reasons for this decision.

Stage 6 – identify privacy risks and solutions

Based on your answers to the questions above, use this section to identify and record privacy risks to the individual. Consider if these are high, medium or law.

Describe the actions you would take to reduce the risks and any necessary future steps and evaluation how effective these actions are likely to be and determinate whether any remaining impact on individuals is justified and proportionate in view of the aims of the project.

Note, if there would be a residual high risk to individual rights and freedoms even after solutions are put in place, you must consult with the ICO before going ahead with the project.

Privacy Issue: Identify potential risk *(two examples are set out below but you need consider the privacy issues for the particular process you are looking to introduce*)	**Risk to individual** Including consideration of likelihood and severity	**Compliance risk:** identify GDPR requirement that may be breached	**Other risk .e.g.** enforcement action, reputational damage, etc	**Solutions** identify how you plan to remove/reduce risk and indicate whether each proposed solution is accepted or rejected	**Risk and evaluation:** is risk eliminated, reduced or accepted? Is final impact on individuals after implementing solution GDPR compliant, justified and proportionate to the aims of the project
Risk of security breach – unauthorised access to data by other employees/managers					
Risk that data retained for longer than necessary					

Stage 7. Consultation with ICO – only if residual high risk

Set out details on information provided to the ICO, advice received and actions taken on that advice.

Stage 8 – Integration of outcomes into project plan

Who is responsible for implementing the solutions that have been approved?

Action	Person responsible	Date for completion	Completed?

Stage 9 – sign off

To be completed by the person with overall responsibility for the project once DPIA solutions have been implemented

Name	Position	Date

Stage 9 Date for Review

DPIAs should be reviewed at least every three years, or sooner if the processing changes.

Review date ……