Privacy impact assessment template

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. The template follows the process which is used in this code of practice. You can adapt the process and this template to produce something which allows your organisation to conduct effective PIAs integrated with your project management processes.

Step one - Identify the need for a PIA :

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

The aim of Beaumont Wood (BW) is to provide professional recruitment and career advice services to a range of candidates and companies, principally in the building products sector. BW intends to perform these services in full compliance with the GDPR.

Individuals will gain suitable employment, and enhancements to their career

Companies will be able to recruit high calibre staff

In pursuance of the above aims data is collected on individual candidates, and potential candidates, from a variety of sources (CV's submitted, LinkedIn, adverts, research and referrals.)

In pursuance of the above aims data is collected on individual companies, and their employees, from a variety of sources (CV's submitted, LinkedIn, adverts, research and referrals.)

Personal details (such as name, contact details, phone numbers, email addresses, residential addresses, date of birth nationality, employment history, remuneration, age and gender) will be collected, retained for a suitable period of time under the "legitimate interest" justification.

Such data will be stored on a cloud based database (provided by Invenias), and on laptop and personal computers used by the Director of BW, and independent contractors employed from time to time. This data will also be stored on a smart phone used by the Director of BW.

The data will be used to identify suitable candidates for vacancies, and potential clients for recruitment services. This would be to the benefit of both sets of individuals.

Other than the data detailed above, there would be no sensitive data ordinarily recorded relating to health, financial details or criminal records. Occasionally data relating to health is sometimes recorded if pertinent to an individual's ability to work.

Individuals are contacted, in a discrete manner, to establish their possible interest in a new role. Usually they are happy for this, if ever they request for no further contact this request is complied with.

There is no use of new technology such as biometrics or facial recognition software. Occasionally clients use psychometric assessments as part of their recruitment process. These reports generated go direct to the candidate, and are not usually stored on the BW system or records.

Step two - Describe the information flows

The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

The data is collected from these sources ((CV's submitted, LinkedIn, adverts, research and referrals.) It is entered into Invenias software. External researchers based in India store data in a Google docs spreadsheet for approval by BW, and this data is then transferred into Invenias.

Approximately 18,500 individuals have their data recorded on the BW Invenias system at the time of writing - March 2018.

Consultation requirements - Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. Consultation can be used at any stage of the PIA process.

In a small organisation with only three active users of the software at the time of writing, consultation has occurred from the Director to the other 2 users. Risks identified as a result of this process have been compiled by the Director.

Step three: identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register. Annex three can be used to help identify the DPA related compliance risks

Privacy issue	**Risk to individuals**	**Compliance risk**	**Associated organisation / corporate risk**
Data breach by hackers	Medium, personal data could be obtained. No financial records are kept.	Risks non-compliance	Reputational, in extremis penalties including fines
Personal data sent to current employer in error	High – current employment status could be jeopardised	Risks non-compliance	Reputational, in extremis penalties including fines
Personal data revealed to another party	Medium, personal data could be obtained. No financial records are kept.	Risks non-compliance	Reputational, in extremis penalties including fines
Smart phone could be lost / accessed by unauthorised person(s). Albeit it is password protected.	Medium, personal data could be obtained. No financial records are kept.	Risks non-compliance	Reputational, in extremis penalties including fines

Step four - Identify privacy solutions

Describe the actions you could take to reduce the risks. And any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems)

Risk	**Solution(s)**	**Result: is the risk eliminated, reduced or accepted?**	**Evaluation: is the final impact on individuals after implementing each solution a justified compliant and proportionate response to the aims of the project?**
Data breach by hackers	Maintain integrity of Invenias software which is password protected. Maintain up to date software, anti-virus software on all relevant computers used	Reduced	Yes

Personal data sent to current employer in error (as a CV)	Only the Director sends out CV's, he is aware of this risk. There are a small number of assignments at any one time, so the risk of confusion is low.	Reduced	Yes
Personal data revealed to another party	All staff and contractors are aware of this risk, and the importance of confidentiality so the risk is low.	Reduced	Yes
Smart phone could be lost / accessed by unauthorised person(s).	Only the Director has a smart phone with this data. It is password protected. Care is taken with its whereabouts. Usually it is kept in a secure office, or if not is on his person or secured under lock and key.	Reduced	Yes

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risks	Approved solution	Approved by
All risks	As above	J M Wood

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork?

Who is responsible for implementing the solutions that may have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns
J M Wood