DPAS

DPIA POLICY

(PART A)

|  |  |  |  |
| --- | --- | --- | --- |
| **Owner** | **Nigel Gooding** | | |
| **Responsible for Delivery Across Data Privacy Advisory Service** | **Nigel Gooding** | | |
| **Version Number** | **V1.0** | **Date** | **12.05.2020** |

**Contents**

1. **Introduction**
2. **Purpose**
3. **Scope**
4. **When Should We Conduct a DPIA?**
5. **Who is Responsible for DPIAs?**
6. **The Stages of a DPIA**
7. **Measure of Policy Effectiveness**
8. **Introduction**
   1. This policy applies to Gooding & Co Ltd, trading as Data Privacy Advisory which is a limited company registered in England and Wales under registration number 10625448 with a registered office at 10 Oaktree Place, Manaton Close, Exeter, Devon. EX2 8WA.
   2. From time to time, we may wish to introduce new systems and/or procedures for various reasons such as improving their services, streamlining processes, assisting staff etc.
   3. DPAS recognises that some of its projects may result in different or additional ways of processing personal data which could be considered intrusive and may give rise to privacy issues or concerns. In such circumstances, certain requirements need to be satisfied. In particular, Article 35 of the General Data Protection Regulation (GDPR) requires a Data Protection Impact Assessment (DPIA) to be conducted where a new or changed way of processing of personal data is likely to result in a high risk to the rights and freedoms of individuals.
   4. The Information Commissioner’s Office (ICO) has issued guidance on Data Protection Impact Assessments and DPAS is committed to following this.
9. **Purpose of Policy**
   1. The purpose of this policy is to provide guidance on completing a Data Privacy Impact Assessment (DPIA). It describes the process for conducting a DPIA through the changes in lifecycle to ensure that, where necessary, personal data, special category personal data and other sensitive information requirements are complied with and risks are identified and mitigated.
   2. The template provided in addition to this guidance is a practical tool to help identify and address the data protection and privacy concerns at the design and development stage of a project or business change, building data protection compliance in from the outset rather than bolting it on as an afterthought.
   3. By following the DPIA process, this will help DPAS assess privacy risks to individuals in the collection, use, storage and disclosure of personal information. A failure to properly embed appropriate privacy protection measures may result in a breach of privacy laws or prohibitive costs in retrofitting a system to ensure legal compliance or address community concerns about privacy.
10. **Scope of Policy**
    1. A Data Privacy Impact Assessment (DPIA) is used to identify any impact on privacy where a new system, service or business process is introduced. A DPIA can also be used to review and assess existing services and systems where changes to the way that personal data is handled are planned. More information of when to complete a DPIA is found in Section 4 below.
    2. This policy applies across DPAS and it is company policy that a DPIA is completed in any of the situations detailed below.
    3. Properly conducted DPIAs will enable DPAS to:
       1. identify and minimise the privacy risks of new projects;
       2. ensure that potential problems are identified at an early stage;
       3. save money by addressing issues before they become complex and costly to resolve;
       4. improve transparency, as individuals will be able to understand how their personal data is being processed;
       5. build confidence in individuals, as they will be reassured that their personal data is being processed lawfully and;
       6. demonstrate to the ICO that all the privacy issues have been carefully considered.
11. **When Should We Conduct a DPIA?**
    1. A DPIA should be carried out whenever there is a change (to either IT or non-IT systems and/or processes) that will introduce a new way of processing personal data or significantly change the way in which personal data is handled. For example, a redesign of an existing process or service, or a new process or information asset being introduced.
    2. DPIAs should be considered in the following circumstances (this list is not exhaustive):
       1. introduction of a new paper or electronic information system to collect and hold personal data;
       2. update or revision of a key process or system that might alter the way in which the organisation uses monitors and reports personal information;
       3. changes to an existing process or system where additional personal data will be collected;
       4. proposal to collect personal data from a new source or for a new activity;
       5. plans to outsource business processes involving storing and processing personal data;
       6. plans to transfer services from one provider to another that include the transfer of information assets;
       7. any change to or introduction of new data sharing agreements.
    3. Any systems which do not identify individuals in any way do not require a DPIA to be performed. However, it is important to understand that what may appear to be “anonymised” data, could in fact be identifiable when used with other information, so anonymised data should be considered very carefully before any decision is made that it will not identify individuals.
    4. Once the initial screening questions in the DPIA template have been answered, it will become clear whether or not a DPIA is required.
    5. Completion of a DPIA should be built into the organisational business approval and procurement processes.
12. **Who is Responsible for DPIAs?**
    1. Any person who is responsible for introducing a new or revised service or changes to a system, process or information asset is responsible for ensuring the completion of a DPIA.
    2. The Data Protection Manager (DPM) and the Data Protection Officer (DPO) should be consulted at the concept stage of any new service, process, purchase or implementation of an information asset so that they can provide advice on the procedures for completing the DPIA.
    3. DPIA outcomes and their mitigating actions must be routinely reported back to the organisation (including the DPO), with risks/issues being recorded and reported through the project/programme board. Significant risks and issues must be raised in order for a risk assessment to be performed.
13. **The Stages of a DPIA**
    1. The flowchart in Appendix A shows the first 7 stages of the DPIA procedure described within this section.
    2. A DPIA should incorporate the following steps:

* Stage 1: Identify the need for a DPIA.
* Stage 2: Describe the processing.
* Stage 3: Consider consultation.
* Stage 4: Assess necessity and proportionality.
* Stage 5: Identify and assess the risks.
* Stage 6: Identify measures to mitigate the risks.
* Stage 7: Sign off and record the DPIA outcomes.
* Stage 8: Integrate the DPIA outcomes back into the project plan
* Stage 9: Update the Data Register / Record of Processing Activity
* Stage 10: Keep Under Review
  1. **Stage 1 – Project Overview and Initial Screening** 
     1. This stage should be completed by the service manager or project lead responsible for delivering the project / proposed change.
     2. Identify the key privacy risks and associated corporate risks on the DPIA template. For large scale DPIAs it may be more appropriate to record this information on a formal risk register.
     3. Any risk of failing to comply with one or more of the GDPR principles should also be recorded. A list of the GDPR principles can be found in Appendix B.
     4. On completion of this stage there will be three possible outcomes:
* The initial screening exercise is incomplete and will have to be repeated or further information obtained.
* The initial screening exercise is complete, and no privacy risks have been identified.
* The initial screening exercise has identified privacy risks and an action plan to mitigate the risks is required.
  1. **Stage 2 – Describe the nature, scope, context and purpose of the processing** 
     1. In describing the nature of the processing DPAS need to explain how the personal data is:
     + collected;
     + used;
     + stored;
     + retained;
     + shared (if applicable) and;
     + deleted.
     1. Those who will be processing the information will need to be consulted on the practical implications and any potential future uses of information should be identified.
     2. In describing the scope of the processing, DPAS need to explain:
* the nature of the personal data;
* the different types of the personal data;
* how much personal data is involved;
  + how sensitive the personal data is and whether it amounts to special category personal data (the definition of special category personal data is set out in Article 9 of the GDPR and is reproduced here in Appendix C)
* how often the processing will take place;
* the extent of the processing;
* how long the personal data will be processed for;
* how many data subjects will be involved; and
* the geographical area covered
  + 1. In describing the context of the processing, DPAS need to explain:
* where and how the personal data was obtained;
* what its relationship is with the data subjects;
  + to what extent the data subjects still have control over their personal data;
  + whether the data subjects are likely to expect their personal data to be processed in this way;
  + whether there are any children or other vulnerable people within the group of data subjects affected;
* whether DPAS has previously done this type of processing;
* whether progresses in technology or security affect the processing;
* any issues of public concern;
  + whether DPAS complies with any relevant GDPR codes of conduct and codes of practice.
    1. In describing the purpose of the processing DPAS need to explain:
  + the reason for this processing ie: what the outcome will be for data subjects;
* what the benefits will be for DPAS and others, if any, and;

if the processing is based on legitimate interests, what that legitimate interest is.

* 1. **Stage 3 – Consider Consultation**
     1. DPAS will need to ensure that it consults with all relevant stakeholders.

This is an important part of the DPIA as it allows interested parties to highlight privacy risks and offer solutions based on their own experience and expertise.

* 1. **Stage 4 - Assess Necessity and Proportionality**
     1. DPAS needs to consider how its plans help to achieve its purpose or if there is another, less intrusive way, to achieve the same result. In particular, DPAS needs to assess whether it is really necessary to carry out the proposed processing and whether it is proportionate to its end goal. As part of this exercise DPAS needs to assess its compliance and record how to ensure that:
  + personal data collected for one purpose will not be used for another purpose (intentionally or accidently);
* the personal data is accurate and up to date;
  + the personal data collected is limited to what is necessary;
* privacy notices are provided to data subjects;
* individuals' rights will be addressed;
  + data processors comply (ie: by using suitably worded contracts) and;
* safeguards for international transfers are put in place.
  + 1. Lawful Basis

DPAS also needs to explain the lawful basis for the processing. There are six legal bases set out in Article 6 of the GDPR.

* + 1. Special Category Personal Data

If DPAS proposes to process special category personal data, they will also need to satisfy a separate condition for processing special category data under Article 9 in addition to identifying a lawful basis under Article 6. Advice should be sought from the DPM and/or DPO in relation to this.

* 1. **Stage 5 - Identify and Assess Risks**
     1. Some privacy issues may have more than one type of risk. For example, it may be a risk to individuals and a corporate risk.
     2. Consider whether there is a Confidentiality, Integrity or Availability of Data Risk (CIA).
     3. DPAS will need to:
* identify and record the privacy risks to individuals;
* assess the risk of reputational damage and loss of public trust;
* conduct a compliance check against all relevant legislation and, in particular, the GDPR, the Data Protection Act 2018, the PECR and the new ePrivacy law (when it comes into force) and;
* keep a record of the identified risks.
  + 1. This process will help DPAS to understand the likelihood and severity of privacy risks.
  1. **Stage 6 – Identify Measures to Mitigate the Risks**
     1. Once the privacy risks have been identified, DPAS will need to:
* devise ways to reduce or eliminate the privacy risks;
* assess the costs and benefits of each approach, looking at the impact on privacy and the effect on the project outcomes and;
* refer back to the privacy risks until satisfied with the overall privacy impact.
  + 1. The above process should take into account the aims of the project and the impact on privacy. DPAS recognises that in some cases, privacy risks will be accepted as necessary for the project to continue.
  1. **Stage 7 – Sign Off and Record the DPIA outcomes**
     1. Once DPAS is satisfied that the DPIA has been successfully completed and all privacy issues addressed, the DPIA will need to be signed off in order for the project to proceed. DPAS should:
* produce a DPIA report;
* consider publishing the report or other relevant information about the process (note: publishing the report is not always appropriate);
* ensure the DPIA is approved at the appropriate level and;
* ensure that the DPIA report or summary is made available to the appropriate stakeholders.
  1. **Stage 8 – Integrate the DPIA Outcomes back into the Project Plan**
     1. After the above process has been completed, DPAS will need to ensure that the outcomes are implemented. DPAS will need to:
* ensure that the steps recommended by the DPIA are implemented;
* continue to use the DPIA throughout the project lifecycle;
* ensure that the privacy solutions are carried out and recorded and;
* ensure the DPIA is referred to if the project is reviewed or expanded in the future.
  1. **Stage 9 – Update Data Register / Record of Processing Activity**
     1. Review and update the Data Register / Record of Processing Activity and data flow models and third-party lists that are impacted by the project. This is essential to keep these materials up to date, so they continue to be an accurate representation of personal data processing.
  2. **Stage 10 – Keep Under Review**
     1. Ensure the DPIA is kept under review as the project develops and progresses and update it as and when necessary.

1. **Measure of Policy Effectiveness**
   1. This policy will be considered effective in situations where DPIAs have been conducted and no breach has occurred since the implementation of the new system or change in way of handling personal data.

# **Document History and Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version No.** | **Author** | **Effective Date** | **Status/Comments** |
| V 1.0 | Sandy May | 07.05.2020 | Published |
|  |  |  |  |

**Review and Approval**

This policy will be reviewed regularly and may be altered from time to time in light of legislative changes or other prevailing circumstances.

|  |  |  |  |
| --- | --- | --- | --- |
| **Reviewer** | **Job Title** | **Signed Off Date** | **Status/Comments** |
| Sandy May | Head of Consultancy | 07.05.2020 | Complete |
| Melanie Garnett | Operations Director | 12.05.2020 | Complete |
| Nigel Gooding | Chief DPO | 12.05.2020 | Complete |

|  |
| --- |
| **Next Review Date** |
| All policies should be reviewed at least annually or when significant change occurs to the policy subject matter.  The next review date for this policy is 20.05.2021 |