****

GDPR006 Data Protection Impact Assessment and privacy by design

**GDPR Toolkit – DPIA:**

Introduction:

This form may be used to support the completion of a DPIA. If you are obligated to complete a DPIA then each step is a requirement of the GDPR. If you are not obligated to complete a DPIA, this form may be used to structure an assessment of your processes and will prompt you to identify aspects of your processes that may need to be re-designed in order to meet the principle of privacy by design and default. This form should be used in respect of each generalised data process, e.g. recruitment, new starter onboarding etc.

For further guidance on this topic, do refer to the appropriate pages on our HR portal.

How to generate your form:

Throughout the form, you will see icons and highlighted areas (see key below). The icons used are for guidance on how to amend the document and should be deleted from the final document, together with any non-applicable optional information/tables.

Key:

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| INFORMATION  This icon demonstrates the text is for information only. | ACTION  This icon means you need to make an amendment to the text. | OPTIONAL  This icon means the advice provided is optional. | WARNING  This icon means the text is important. Please take note of the advice. |

Any text you find highlighted should be amended to suit your customisations and/or removed from the document.

Customising your form:

In addition to the text emphasised with icons and highlights, you can also amend the font, margins and footer information to suit your needs.

All fonts used throughout the document are set in the Styles panel (under the Home Tab in Word 2007+). To change the font settings, right click on the style and click M*odify*. Make the appropriate changes and click OK. Your document will automatically update wherever that style is used.

To remove the icons, click on them and press delete.

You will find a checklist of customisations at the end of the document. Please run though this once you have completed your customisations. You will also need to **delete this page by clicking Insert -> Cover Page -> Remove Current Cover Page.**

GDPR006 Data Protection Impact Assessment and privacy by design

|  |  |
| --- | --- |
| Tracker | |
| Department: |  |
| Process: |  |
| Date completed: |  |
| Completed by: |  |
| Controller: |  |
| <Optional:> DPO: |  |





|  |  |  |
| --- | --- | --- |
| 1. Purpose   A clear statement of the purpose for collecting and/or processing personal data. | | |
|  | | |
|  | | |
| 1. Legal basis   The lawful basis the relied upon to process the personal data. | | |
|  | | |
| Legal bases | **Tick if applies** | **Justification** |
| Contractual Obligation |  | (Identify the title and date of the applicable contract.) |
| Consent |  | (Ensure that you obtain consent in line with GDPR conditions in advance of the processing.) |
| Legal Obligation |  | (State the requirement and the legislation applicable.) |
| Vital Interest of Data Subject |  | (This will only apply in exceptional circumstances e.g. critical medical emergencies.) |
| <Optional:> Public Interest |  | <This will only apply in exceptional circumstances e.g. whistleblowing, you are a public body and/or meet relevant conditions etc.> |
| Legitimate Business Requirement |  | (Eg a genuine and necessary business function.) |
| 1. Proportionality | | |
| Explanatory note  Only data that is necessary and relevant to achieve the purpose should be collected. Assess whether all the data you collect, intend to collect, or process will be for a specified, explicit and legitimate reason. Note: Special category data is prohibited subject to limited exemptions under Article 9 of GDPR which include: the data is necessary for employment; or the data subject has given explicit consent. | | |
| Type of personal data required (eg name, d.o.b, contact details, special category info e.g. medical details, ethnicity, biometric data etc.) | **Justification**  (in relation to the purpose) | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
|  |  | |
| 1. Process | | |
| Explanatory note  A step by step account of the processes used to obtain, store and remove personal data. Processes must incorporate:   * Data security by design – you must evidence both technological and organisational measures. * Storage limitation – data must not identify an individual for any longer than is necessary. * Measures to maintain accuracy – data must be kept up to date (proportionate to the purpose). | | |
| Who is affected | | |
| Who are the data subjects? |  | |
| How many data subjects may be affected? |  | |
| Who are the recipients? |  | |
| Are any third parties involved? |  | |
| Collection | | |
| Who collects the data? |  | |
| What format do they collect the data in? |  | |
| How is the data moved from the point of collection to where it needs to be? |  | |
| Processing | | |
| Describe step by step what happens once data is obtained. | * <<text>> * <<text>> * < * < * text>> | |
| Retention | | |
| How is it saved? |  | |
| What is the location? |  | |
| Who has the potential to access it? |  | |
| Who requires access? |  | |
| What measures are in place to ensure access is restricted? |  | |
| How else is the information controlled? |  | |
| List everything the information may be accessed for. Does this match the ‘purpose’? |  | |
| Is there a legitimate reason to save the data for any period of time? |  | |
| How long will the data be stored for? (Specify if any data will be kept for different lengths of time.) |  | |
| Could the data be pseudonymised? |  | |
| How is the data kept up to date (with regard to the purpose?) |  | |
| How is the data subject informed of the update? |  | |
| Erasure | | |
| How is the data deleted? |  | |
| Is this secure? Explain. |  | |
| Is the data irrevocable? If not what is the lawful justification? |  | |
| How do you record deletions? |  | |
| Are data subjects notified of any erasure or updates? |  | |
| Reliance on Consent | | |
| How do you gain consent? |  | |
| How do you record evidence of consent? |  | |

|  |  |
| --- | --- |
| 1. Risks   An assessment of the risks to data security and the right and freedoms of the data subjects. | |
|  | |
| Privacy Risks  Consider the extent of possible circulation and identification of a data subject. | |
| Which points in the process is data potentially vulnerable? |  |
| How do you identify privacy risks? |  |
| How do you currently address risks identified? |  |
| Security Risks  Consider the extent to which personal data is protected against loss, theft, loss of access and destruction. Consider both physical and cyber security. | |
| Which points in the process will data potentially be unsecure? |  |
| What security is currently in place? (eg alarms, locks) |  |
| Rights and freedoms  Consider whether any right or freedoms are jeopardised, particularly those listed below. | |
| Right of transparent communication |  |
| Right of access |  |
| Right to rectification (and obligation to notify recipients) |  |
| Right to erasure (right to be forgotten) |  |
| Right to restriction of processing |  |
| Right to data portability |  |
| Right to object |  |
| Right to not be subject to automatic decision making |  |
| Freedom of speech, thought, movement. |  |
| Right to equality, liberty and conscience. |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Potentially significant or high risks** | | | | | | | | | | | |
| **Issue** | Risk to rights and freedoms | Compliance Risk | Access by unauthorised third parties | Risk of loss of access to data | Risk of damage | Risk of theft | Risk of destruction | What are the potential ramifications? | What is the likelihood? | Can measures eliminate or reduce risk? | **Evaluation**  (The final assessment of risk) |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |
| --- | --- |
| 1. Measures   These must include technological and organisational security measures which protect rights and freedoms and implement the principles of data protection laws. | |
|  | |
| List the technological measures in place to ensure privacy and security in this process?  (This correlates with the ‘solutions’ in previous section.) |  |
| List the organisational measures in place to ensure privacy and security in this process?  (This correlates with the ‘solutions’ in previous section.) |  |
| Do staff know who to report a breach to? |  |
| Have appropriate safeguards been integrated? |  |
| Are they state of the art? If not, explain justification. |  |
| Have safeguards been tested? |  |
| Is processing designed so that only necessary personal data is collected by default? Explain. |  |
| Have any unjustifiable retention periods been modified and communicated? Explain. |  |
| Is there certainty that personal data cannot be made available to an indefinite number of people? |  |
| Are staff aware of where the privacy and security risks are which are relevant to their job? |  |
| Have staff been trained appropriately? |  |
| What training have they received? |  |
| How will evidence of satisfactory training be recorded? |  |
| How will awareness be maintained? |  |
| What is the rationale that will determine the next review of processing? |  |
| <Optional: In the interest of the transparency principle, and where appropriate, the views of the data subjects may be sought regarding the processing.> 7. Views | |
|  | |
| Is it appropriate to solicit the views of the data subjects? |  |
| Who should be consulted about the processes? |  |
| How will views be collected? |  |
| How will this be saved? |  |



|  |  |
| --- | --- |
| Sign Off | |
| Approval on behalf of the processor | |
| Approval of processor required | Yes No |
| Representative of processor: NAME |  |
| Representative of processor: SIGN |  |
| DATE |  |
| Approval on behalf of the controller | |
| Representative of controller: NAME |  |
| Representative of controller: SIGN |  |
| DATE |  |
| Review Date |  |

Checklist

Upon completion of customisations please ensure you have:

* customised all relevant text and removed pink highlighted text
* removed all icons
* diarised a reminder to review and update the form
* removed the front cover (see instructions on front cover)
* removed this checklist!