**Data Protection Impact Assessment**

**Objective**

The purpose of a data protection impact assessment (DPIA) is to assess and demonstrate compliance with data protection legislation. The DPIA also provides evidence that the risks to individuals have been considered and sufficient measures have been taken to protect those individuals. The DPIA should assess the activity to be carried out against all the principles of data protection and determine whether the processing of personal data is both necessary and proportionate or whether changes to the process or additional controls are required.

|  |
| --- |
| **Instructions**   * This DPIA template is provided only for ethics review applications submitted to CIREP. Please check CIREP’s application procedures before filling out this form. * First complete the ethics checklist, which will help you determine whether you need to fill out the DPIA. If that is the case: * You should complete all of the sections in this template and enclose the document (editable version) with your CIREP application to receive feedback on any risks identified and recommendations on the actions or controls needed to address those risks. * Do not delete the instructions in blue (unless they are between square brackets), or any section. Write “not applicable” if an item or a question does not apply to your project. Delete the examples that do not apply. * **Skip section 5**, on personal data protection, **in the protocol form**. * It is the responsibility of the principal investigator (PI) to ensure the required controls are put in place and to sign off on any risks arising from the processing. * The DPIA should be updated to reflect any changes to the processing as the project or activity progresses. |

**General Information**

|  |
| --- |
| Project Title: |
| PI Full Name: |
| Date: |

**1. Study Details**

|  |
| --- |
| Why is the use of personal data necessary for this activity? |
| Who will benefit from the activity? |
| Could the use of personal data for this activity result in any harm to the individual? Provide detail. |
| If the activity involves processing personal data on a large scale, provide detail. |
| If the activity involves matching or combining datasets, provide detail. |
| If the activity involves data concerning vulnerable individuals or children under 14, provide detail. |
| If the activity involves new, or innovative uses of, technological or organizational solutions, provide detail. |
| If the activity could prevent individuals from exercising a right, using a service, or fulfilling a contract, provide detail. |
| Any other information in respect of the study which may be relevant (maximum 300 words) |

**2. Personal Data**

List the types of personal data that will be **collected**, **used**, **accessed**, or **shared** for the purpose of this activity, and the granularity/level of detail of the data.

|  |  |  |
| --- | --- | --- |
| Data Collected | Justification | Processing Activity |
| **Example:** *Participant names (indicate if this includes full name, initials, etc.)* | *Identification so that we can apply matching codes across longitudinal data sets* | *Excel database located x Drive on x desktop computer at x site* |
| **Example:** *Written consent* | *Legal basis for processing* | *Paper forms stored in a locked filing cabinet at x site. Access restricted to [detail] only* |
| **Example:** *Political beliefs and education level (indicate the scale for political belief, the levels for education level)* | *Needed because the project aims to correlate these variables* | *Google forms created from an @upf.edu account. Access restricted to [detail] only* |
|  |  |  |
|  |  |  |

**3. Transparency of Processing**

|  |
| --- |
| How will you notify participants about the data processing that will be carried out using their personal data? |

**4. Data Security: Storage and Sharing**

|  |
| --- |
| Describe in detail the technical and organizational security measures that will be applied to protect personal data including, but not limited to, access controls, data sharing restrictions, encryption, pseudonymization, anonymization, etc. |

**5. Data Minimization**

|  |
| --- |
| Have you ensured that you will only collect the minimum data that you need or that is necessary for the activity? Provide details. |

**6. Lawful Basis: Personal Data Processing**

If processing personal data, you must satisfy at least one of the lawful bases as set out under [Article 6 GDPR](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1797-1-1). Note that personal data processing for research purposes is typically based upon the data subject’s consent.

|  |  |
| --- | --- |
| Legal Basis  for the Personal Data Processing | Details |
| Consent | *[Describe the consent documentation and storage procedures.]* |
| Performance of a contract or an agreement | *[Provide detail.]* |
| Legal obligation | *[Please specify.]* |
| Public interest or exercise of official authority of a public institution | *[Please specify.]* |
| Vital interests of data subjects | *[Provide detail.]* |
| Legitimate interests of a private company | *[Provide detail.]* |

**7. Lawful Basis: Special Categories of Personal Data**

Processing special categories of personal data includes the following:

* processing personal data revealing
* racial origin,
* ethnic origin,
* political opinions,
* religious beliefs,
* philosophical beliefs, or
* trade-union membership;
* processing genetic data for the purpose of uniquely identifying a natural person;
* processing biometric data for the purpose of uniquely identifying a natural person;
* processing data concerning health;
* processing data concerning a natural person’s sex life;
* processing data concerning a natural person’s sexual orientation.

If processing special categories of personal data, in addition to the Article 6 lawful basis, you must also satisfy one of the following conditions as set out under [Article 9 GDPR](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1797-1-1). Note that processing of special categories of personal data for research purposes is typically based on explicit consent.

|  |  |
| --- | --- |
| Legal Basis for the Processing of Special Categories of Personal Data | Details |
| Explicit consent | *[Describe the explicit consent documentation procedures.]* |
| Authorized by law | *[Please specify.]* |
| Vital interests of the data subject or another person | *[Provide detail.]* |
| Carried out (internally) by a not-for-profit organization with a political, philosophical, religious, or trade union aim | *[Provide detail.]* |
| Information that has already been made public by data subject | *[Provide detail.]* |
| Necessary for the establishment, exercise, or defense of legal claims | *[Provide detail.]* |
| Necessary for substantial public interest | *[Provide detail.]* |
| Necessary for reasons of public interest in the area of public health | *[Provide detail.]* |
| Archiving purposes in the public interest/scientific or historical research purposes/statistical purposes | *[Provide detail.]* |

**8. High-Risk Processing**

Does the research involve any of the following?

* evaluating or predicting outcomes in individuals;
* decision-making by automated means, e.g., using algorithms;
* monitoring the behaviors of individuals;
* the surveillance of individuals, use of location, or the use of biometric technology such as facial recognition.

|  |
| --- |
| If so, provide details and describe the impact to the individuals. |

**9. Internal Data Sharing**

|  |
| --- |
| Will the personal data be shared internally (i.e., within UPF)? If so, provide details on the data sharing including information on the necessity for the processing, the format of the data that is to be shared, with whom the data will be shared, and confirmation of the security measures in place to protect the data in transit. |

**10. Third Parties**

|  |
| --- |
| Will the personal data be shared with third parties, including IT service providers, cloud-based solutions, subcontractors, etc.? If so, provide details including information on the contractual arrangements in place and confirm what due diligence has been carried out. |

**11. International Data Transfers**

|  |
| --- |
| Will the personal data be transferred or stored outside the European Economic Area (EEA) at any point or placed with cloud providers that store data outside the EEA?[[1]](#footnote-1) If so, provide details. Have you ensured that suitable conditions for transferring the data are in place? Provide details or state if unsure. These include:   * adequate jurisdiction, * standard contract clauses, * binding corporate rules, * authorization from the Data Protection Authority. |

**12. Data Retention**

|  |
| --- |
| How long will the personal data be retained for and why? Provide details and explain why a shorter retention period would not be appropriate for your research project. |

**13. Data Subject Rights**

|  |
| --- |
| What plans are in place for responding to a request from an individual in relation to their data protection rights? These include:   * right of access, * right to rectification, * right to erasure, * right to object to processing based on legitimate or public interest, * right to data portability, * right to object to profiling or making decisions about individuals by automated means. |

**14. Training**

|  |
| --- |
| What guidance and training will be provided to individuals involved in this project or activity to enable them to understand their data protection responsibilities? Provide details. |

**15. Processing Risks**

**15.1. Examples**

In the table below (15.2), describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.

Different projects carry different risks and these should be considered. Some examples of privacy risks are given below, but this list is not exhaustive:

**Risks to individuals**

* Hacking of computers where project data is stored.
* Loss of a storage device where project data is stored (e.g., USB drive or laptop).
* The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people’s knowledge.
* New surveillance methods may be an unjustified intrusion on their privacy.
* Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
* The sharing and merging of datasets can allow organizations to collect a much wider set of information than individuals might expect.
* Identifiers might be collected and linked which prevent people from using a service anonymously.
* Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
* Collecting information and linking identifiers might mean that an organization is no longer using information that is safely anonymized.
* Information that is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
* If a retention period is not established, information might be used for longer than necessary.

**Compliance risks**

* Non-compliance with the common law duty of confidentiality.
* Non-compliance with the General Data Protection Regulation or Spanish Organic Law 3/2018.
* Non-compliance with ENS (Spanish National Security Schema, defined in Royal Decree 3/2010).
* Non-compliance with other applicable legislation.

**Associated organization/corporate risks**

* Non-compliance with the data protection or other legislation can lead to sanctions, fines, and reputational damage.
* Problems which are only identified after the project has launched are more likely to require expensive fixes.
* The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organization.
* Public distrust about how information is used can damage an organization’s reputation and lead to loss of business.
* Data losses which damage individuals could lead to claims for compensation.

**15.2. Table**

Complete the table.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk Detail | Risk Rating (High, Medium, Low) | Solutions/Mitigating Actions | Effect | Outcome |
| **Example:** *Hacking into computers where project data is stored.* | *Low* | *All computers storing data are password protected. The external hard drive and remotely accessible computer are also encrypted and locked in an office (on UPF’s campus). Access is restricted to designated staff only.* | *Reduced* | *Low* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**16. IT Security Measures**

The Spanish Royal Decree 3/2018, regulating the National Security Framework in the area of e-Government (Esquema Nacional de Seguridad [ENS])[[2]](#footnote-2) provides the following categorizations:

|  |  |
| --- | --- |
| A data breach in [dimension] may cause… | ENS Categorization |
| Null or negligible inconveniences | Not applicable (N/A) |
| Inconveniences that can be overcome with some difficulties: increased costs, lack of understanding, stress, physical damage, inability to access a service, etc. | Low |
| Significant difficulties: discrimination, identity theft, financial loss, psychological damage, damage to reputation, physical harm, deteriorating health, loss of employment, etc. | Intermediate |
| Irreversible consequences that may not be overcome: death or serious physical or psychological damage, etc. | High |

This categorization shall be applied to each of the five security dimensions defined by ENS. IT security officials use the categorization to determine the specific security measures to be applied to a particular automated data processing.

Complete the table by specifying the appropriate ENS category. Options: N/A, low, intermediate, high.

|  |  |
| --- | --- |
| Dimension (definition) | ENS Categorization |
| Availability (inability to access the service) |  |
| Authenticity (inability to guarantee the origin of the data) |  |
| Integrity (inability to guarantee non-authorized modification of data) |  |
| Confidentiality (inability to guarantee non-authorized access to the data) |  |
| Traceability (inability to duly assign an entity being responsible for an action) |  |

The ENS categorization is specific to the Spanish public sector. International information security standards include ISO/IEC27001, SOC2, HIPAA, and others. International projects or subcontractors may be certified according to these standards.

|  |
| --- |
| If this is the case, please provide information on the international information security standards followed by your project or your subcontractors. |

**17. Data Protection Officer’s Opinion**

|  |
| --- |
| [To be completed by UPF’s Data Protection officer] |

**18. Disclaimer**

The material contained in this guidance contains general information and guidance only. Please note that this guidance does not constitute legal advice and is provided for general purposes only. Neither is it intended to provide a comprehensive or detailed statement of the law.

No liability whatsoever is accepted by Universitat Pompeu Fabra for any action taken in reliance on the information contained in this guidance. You should not act or refrain from acting on the basis of any information provided in this guidance but rather you should always seek specific legal or other professional advice. Any and all information is subject to change without notice.

1. EEA is made up of the EU 27, Iceland, Norway, and Liechtenstein. [↑](#footnote-ref-1)
2. Applicable to all personal data processing conducted by a public institution in Spain (First Additional Disposition of Organic Law 3/2018, on personal data protection and digital right guarantee). Most research projects have N/A or low categorization on all ENS dimensions. Please ask your IT support staff if you have questions while completing this table. [↑](#footnote-ref-2)