**Data PrOTECTION Impact AssessmentS GUIDANCE**

**This guidance explains when a data protection impact assessment (a DPIA) will be necessary to carry out, and how to carry it out.**

**Any project or activity proposed to involve the processing of personal data should have a designated Information Asset Owner. Information Asset Owners are responsible for assessing information security and privacy risks annually for their assets and implementing appropriate measures accordingly. Accordingly, the Information Asset Owners are responsible for completing a DPIA in respect of the relevant project or activity in accordance with this guidance.**

**What is a DPIA?**

A DPIA is a structured method by which you can understand the privacy risks associated with the processing of personal data and how to take appropriate steps to manage those risks. It is a process to build and demonstrate compliance with data protection legislation.

**What is personal data? What is sensitive personal data (or special categories of data)?**

Personal data is “any information relating to an identified or identifiable natural person (referred to as a “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. So, some obviously personal data are name, contact details (post, phone, e-mail etc.), relationship, educational and financial details. Less obviously personal data are IP addresses and device IDs, pseudonymous data (e.g. hashed or encrypted data).

In addition, personal data has a sub-set known as ‘sensitive personal data’ or ‘special categories of data’. These are data relating to a data subject’s:

• racial or ethnic origin

• political opinions

• religious or philosophical beliefs

• trade union membership

• genetic data

• biometric data for the purpose of unique identification

• health

• sex life or sexual orientation

**Why should I carry out a DPIA?**

From 25 May 2018, the Data Protection Act 1998 will be replaced with the General Data Protection Regulation (**GDPR**). Under Article 35 of GDPR, DPIAs will become **mandatory** for certain processing and all activities “likely to result in high risk to individual”’ data. These activities can include:

* Use of new technology
* Large scale processing of sensitive personal data
* Systematic and extensive evaluation of personal data which may result from profiling or automated decision making

Even where a DPIA is not a mandatory requirement, it will remain best practice for any process which might involve the handling of personal data e.g. a new database or survey involving staff or student data or if a new supplier is being procured.

DPIAs will show that the College has taken into account the data protection principles and will help us to comply with the GDPR requirements to “implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation.”

A DPIA does not need to be a lengthy process – you may carry out the first step and discover you do not need to carry out a full DPIA. If a full DPIA is required, the assessment itself is fairly straightforward.

The benefits of a DPIA are:

* enhancement of informed decision making, especially with regards to data privacy risks;
* evidence of legal and regulatory compliance and an audit trail to show you attempted to prevent privacy risks;
* enhancing trust and confidence in your work from stakeholders by showing you take data privacy, and transparency seriously; and
* efficiency of your project by identifying privacy risks and solutions early on.

**Failure to comply**

Failure to carry out a DPIA, or carrying one recklessly or carelessly (e.g. where material information is omitted or misrepresented) notwithstanding any subsequent data protection breaches, will be subject to a potential fine by the regulator of up to €10 million or 2% of an organisation’s annual turnover – whichever is the greater.

In addition to this, data subjects whose personal data has been compromised will be able to pursue legal action against the organisation found to have compromised the data, and of course, there is the risk to reputational damage.

**How do I carry out a DPIA?**

**The DPIA Template** sets out an initial list of screening questions which should be considered at the start of a project/activity/research proposal/supplier relationship where personal data will or is likely to be involved in any way. If the answer is ‘yes’ to any of these questions then a DPIA is likely required though please contact the College’s Data Protection Officer (robert.scott@imperial.ac.uk) where this can be discussed and further guidance sought. Even if the answers are all ‘no’ but you will be processing personal data, then you should still consider carrying out a DPIA as it is best practice to show that we are complying with the legislation.

A DPIA should be conducted at the beginning of any proposal that will lead to data processing and be reviewed at least every 3 years, or more frequently, taking into account the nature of the processing and the rate of any changes or modifications made to it or the system it uses.

If an existing use of technology is likely to change after 25 May 2018, or we intend to use a different supplier after this date, then a DPIA should be carried out now to assess the new risks. A DPIA should be reviewed regularly throughout the lifecycle of a project, helping you to identify risks and ensure compliance throughout. It should be seen as a continuous process, not simply a one-time report.

Before carrying out a DPIA, you should identify relevant stakeholders who should be consulted for the purposes of the assessment. These stakeholders may include:

* the people who understand the initiative and any predecessors from a technical and information point of view;
* the people who will be using the new system;
* the people whose information will be processed by the new system - it may be difficult to reach the people whose data will be processed by any proposed new system but you must consider whether there are existing methods of contacting them (or a representative group) for consultation. For example, the College’s Data Protection Officer could represent their views, or you could consider inviting sample participation groups or speaking to the Students’ Union;
* the people who have responsibility for data protection and information security within College;
* collaborative partners;
* the suppliers of a system.

The Data Protection Officer (in consultation with others as appropriate) will carry out periodic compliance audits of departments as well as of completed DPIAs and any non-compliance will be reported to the College’s Information Governance Steering Group (**IGSG**) in the first instance with the IGSG being able to further report to the Audit Committee.

Please note that the College may disclose completed DPIAs where it is required to do so by law (including the Freedom of Information Act), by any applicable governmental or other regulatory authority, or by order of a court.

[*notes on how to complete the different sections of the DPIA follow below*]

**COMPLETING THE DATA PROTECTION IMPACT ASSESSMENT**

**Step 1 – DPIA Summary**

This step involves explaining/understanding/providing the reasoning behind the processing and will document the background and reasons that the processing will be carried out.

**Step 2 – Identifying the need for a DPIA**

Completion of the questions will form the basis of potential risks and identify whether a full DPIA will be required.

**Step 3 – Describing the Data Processing**

At its simplest, this requires consideration of:

* what personal information is to be processed;
* is it absolutely necessary to have that personal data for the purposes of the project;
* is the potential risk to the data subject of processing their data justifiable;
* who will have access to it;
* what it will be used for; and
* how long it will be kept.

In order to gather the necessary use case and technical information necessary for this step, it is likely that consultation with at least some of the stakeholders will be necessary. This is therefore the part of the DPIA process where the consultation begins.

**Step 4 – Legal basis for processing**

The College must have one of six prescribed lawful bases for processing personal data. Seeking consent from the individuals whose data that are is one basis for processing but should be considered only where there is no more suitable legal basis for the processing.

The six lawful basis are:

(i) processing is permitted if it is necessary for the entry into, or performance of, a contract with the data subject or in order to take steps at his or her request prior to the entry into a contract (in short, there is contractual necessity);

(ii) processing is permitted if it is necessary for compliance with a legal obligation under EU law or the laws of a Member State (in short, where the College has to comply with a UK or EU law legal obligation);

(iii) processing is permitted if it is necessary in order to protect the vital interests of the data subject or of another natural person (in short, to protect vital interests);

(iv) processing is permitted if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller under UK or EU/ EU Member States law (in short, the public interest basis) – this would be relevant for some functions carried on by the College such as teaching and research in the public interest);

(v) processing is permitted if it is necessary for the purposes of legitimate interests pursued by the controller (or by a third party), except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects which require protection, particularly where the data subject is a child (in short, the legitimate interest basis).

Note that the legitimate interest basis does not apply to processing carried out by public authorities in the performance of their duties i.e. the College cannot use this basis with respect to activities that are carried out in the public interest such as teaching and research in the public interest;

(vi) processing is permitted if the data subject has consented to the processing (i.e. with consent).

Consent must be unambiguous, verifiable (we ought to document proof of consent), distinguishable from other matters (e.g. other terms and conditions), easy to withdraw, (generally) must not be conditioned on access to a service. Silence, inactivity and pre-ticked boxes do not amount to consent.

Not only that the standard of valid consent under the GDPR is high but also if we seek consent to the processing of personal data, the individuals who have consented will also be able to exercise the right to erasure and the right to portability more easily.

In addition to carrying out the above analysis and choosing one of the six lawful basis for processing, if it is proposed to process any sensitive personal data (also known as special categories of data), you must also satisfy one of ten additional grounds which are as follows:

* the processing is necessary for the establishment, exercise or defence of legal claims, or for courts acting in their judicial capacity;
* the processing is necessary in the context of employment law, or laws relating to social security and social protection;
* the processing is necessary for reasons of substantial public interest, and occurs on the basis of a law that is, inter alia, proportionate to the aim pursued and protects the rights of data subjects;
* the processing is necessary to protect vital interests of the data subject (or another person) where the data subject is incapable of giving consent;
* the processing is necessary for the purpose of medical treatment undertaken by health professionals, including assessing the working capacity of employees and the management of health or social care systems and services;
* the processing is in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, former members, or persons with whom it has regular contact in connection with its purposes;
* the processing is necessary for reasons of public interest in the area of public health (e.g., ensuring the safety of medicinal products);
* the processing relates to personal data which have been manifestly made public by the data subject;
* the processing is necessary for archiving purposes in the public interest, for historical, scientific, research or statistical purposes, subject to appropriate safeguards;
* the processing is carried out with the explicit consent of the data subject.

Note that your choice of lawful basis for processing personal data (the one of six bases) does not dictate which special category condition (the one of ten conditions) you must apply, and vice versa. For example, if you use consent as your lawful basis for processing personal data, you are not restricted to using explicit consent for special category data processing. You should choose whichever special category condition is the most appropriate in the circumstances – although in many cases there may well be an obvious link between the two.

**Step 5 – Describe the information flow**

This step involves a visualisation of the data lifecycle

The desired outcome of this step is to have a detailed description of the proposed information flows that is:

* sufficiently thorough and detailed to act as a solid basis for identifying potential privacy risks; and
* presented in a form that is comprehensible to the stakeholders.

You should therefore be careful to avoid too simplistic representation of the information flows. Try to ensure that every aspect of the data gathering, storage, processing, transmission, analysis, sharing, archiving and disposal is fairly captured if it has a realistic potential for affecting the privacy of individuals.

This stage can be complicated by several factors, for example:

* the precise nature of the information, what it will be used for and the people who will have access to it could be quite open ended;
* it might be necessary to take account of the potential for unintended access to the data, particularly if it is being stored, processed or transmitted outside the institution, or accessed through mobile devices; and
* the data might be used differently in the future to how it is expected to be used at the outset.

Many projects will already have much of this information as a result of the analysis work necessary for the project design. If so, there is no need to re-invent the wheel.

There is no set format for presenting this information – the most appropriate form could be different for each project or activity, but could include narrative, process diagrams or other illustrations or any combination of these in scenarios where the example given in the template is not adequate.

**Step 6 – Data Processor / Contractor requirements**

When the College will be utilising a third party company, contractor and/or supplier to carry out processing on its behalf the GDPR dictates that the College must ensure all parties are aware of their legal responsibilities and these are recorded to ensure complete transparency. This could be achieved within the terms and conditions of the agreed contract, a data processing or sharing agreement or ensured via other recorded agreements documented by the parties.

Furthermore, in instances when personal data will be transferred outside of the EEA this will require further checks/actions to ensure compliance is documented/achieved.

**Step 7– Identify the privacy and related risks**

This is in many respects the core of the DPIA process.

The aim of this step is to compile a comprehensive list of all the privacy risks associated with the initiative, *whether or not those risks require action by the project*.

There is a temptation at this stage to include only those risks likely to have a material bearing on the initiative, and to exclude risks that have already been addressed in the proposed system.

For example, a project involving a new cashless payments element involves a risk that users’ card details could be ‘hacked’. This risk should be included even though it has already been established that the service provider is PCI-DSS compliant.

Similarly, any risks identified by stakeholders during the consultation should be included, even if they turn out to be groundless. For example, a project to implement a new contactless access control system might solicit the concern that it could read private information on peoples’ mobile phones. Although this concern may turn out to be based on a misconception about the technology involved, excluding it from the list of risks could be seen as undermining the process of consultation.

Anyone who has engaged with the consultation process deserves to have their concerns listened to and addressed.

This step requires considerable understanding and imagination to identify the less obvious risks, and the author of the PIA should be prepared for additional risks being highlighted during subsequent steps.

For each privacy risk identified there should be:

* a unique identifier;
* a short title;
* an explanation of the risk that is readily comprehensible by all the stakeholders;
* an assessment of the impact of the risk as it affects individuals;
* an assessment of the impact of the risk from a compliance perspective (from the institution’s perspective) (see the data protection principles below).

You should consider how to capture the risks identified as part of the DPIA process in existing risk management frameworks that you are using.

As an example, the following risk could arise from a project to move from an in-house hosted student records system to the supplier’s SaaS offering.

| **Risk ID/Ref.** | **Risk title** | **Risk explanation** | **Potential impact on individuals** | **Compliance impact** |
| --- | --- | --- | --- | --- |
| SRS-PIA-007 | Data intercepted in transit | Information entered into or retrieved from the student record system will need to traverse the internet between the user’s PC or mobile device and the supplier’s datacentre. This will involve transmission over parts of the internet over which neither the University nor the supplier have control. There is a risk that the information could be intercepted in transit, revealing personal information to third parties. | Personal, sensitive or confidential information may be used for unauthorised purposes or disclosed inappropriately. | Organisation might be in breach of GDPR principle 6.  Reputational damage, cost of defending prosecution, possible fines.  University information may be used for unauthorised purposes or disclosed inappropriately. |

When identifying possible risks which will arise from the processing of personal data, you should consider the data protection principles which are set out in Appendix A. This will ensure that you are analysing privacy risks from the view of the data subject and not from the College’s perspective. This will also help to identify the impact on our compliance with GDPR, and the subsequent business impact on the College.

**Step 8 – Identify privacy solutions**

This is where solutions are identified for the risks.

The aim is to identify, for each of the privacy risks listed in Step 2, sufficient solutions to eliminate the risk or reduce it to a level that is acceptable by the institution.

For some identified risks, no solution is required because the likelihood is so low or the impact so small that it is already acceptable to the organisation. Most identified risks, however, will need some action to eliminate or render them acceptable, and in some cases, there could be more than one solution identified.

Continuing the example in Step 7:

| **Risk ID/Ref.** | **Risk title** | **Solution(s)** | **Action required** | **Result: is risk eliminated, reduced or accepted?** |
| --- | --- | --- | --- | --- |
| SRS-PIA-007 | Data intercepted in transit | 1. The supplier’s datacentre has a direct connection to the Janet network.  2. The traffic between the client device and the servers is encrypted using https. | None | The risk is reduced to the level where it is accepted |

The solutions here illustrate three points:

* The supplier’s direct connection to the Janet network will certainly reduce the likelihood of traffic interception between on campus users and the datacentre, and because this is the most common use case, the solution is good news. However, it will do nothing to prevent interception for off-campus users, as they will be using other networks. This demonstrates the importance of having a thorough understanding of the use cases and information flows.
* The use of https encryption might be thought of as eliminating the risk altogether. Certainly, given the current state of technology, it would reduce the risk to a very low level indeed.
* Neither of the identified solutions requires the College to take any action – both are ‘built in’ to the proposed system. Not all privacy solutions require actions to be added to the project plan.

The solutions may take many forms, for example:

* No solution necessary – the risk is based on a misconception or is so unlikely to be realised (or so minimal in impact) that it is acceptable with no further action.
* A contractual arrangement between the supplier and the College will provide the additional assurance necessary.
* A fair processing notice and opt-in approach can inform users about how their data will be used and give them the opportunity to positively record their agreement to participate.
* A policy can be introduced to reduce the risk to an acceptable level.
* Operational procedures might be introduced to manage the risk.
* Certain features in the product can be disabled.
* A training programme could be deployed to make people aware of the risk and the actions to take to avoid it.
* Technical measures, such as the enforced use of strong encryption, could be built into the project to reduce the risk.
* As a last resort when no other solutions are available, the initiative may have to be abandoned. Alternatively, we may need to approach the regulator, the Information Commissioner’s Office on our proposed use of personal data here.

The solutions identified need to be acceptable to the institution, both in terms of reducing the risks to acceptable levels and in terms of not fatally undermining the business case for the initiative. The solutions will also need to be acceptable to all the other stakeholders.

Remember that for each risk, it may be appropriate to deploy several solutions in parallel. You may also need to be flexible in how you use the table. A risk may have multiple solutions, a solution may have more than one action, and several risks could share the same solutions and actions.

**Integrate the solutions into the project/activity plan**

A DPIA is not a box ticking exercise. Any identified actions need to be built into the project plan and progress has to be monitored by the Information Asset Owner. If any approval is granted on the basis that certain actions are to be taken by a set deadline and those actions are not completed by that deadline, the Information Asset Owner should bring this to the attention of the approvers and suggest appropriate remedial action.

**Step 9 – Sign off / Approvals**

At the end of the assessment, the DPIA with the proposed solutions should be signed off as follows:

***Sign off by the Information Asset Owner:***

1. where only the screening questions have been completed and a full DPIA is not required to be completed on this basis; or
2. where the full DPIA has been completed and satisfactory solutions have been found to any identified risks;

and, in each case, (i) no sensitive personal data is proposed to be processed as part of the project or activity and (ii) the project or activity will not involve the processing of personal data about 250 or more individuals,

the Information Asset Owner is authorised to sign off the completed DPIA in consultation with the local Data Protection Co-Ordinator (if one has been nominated).

Where the Information Asset Owner is uncertain as to whether he/she is able to sign off on a given DPIA or uncertain about any GDPR compliance aspects, he/she should contact the College’s Data Protection Officer for further guidance.

***Sign off by the Information Asset Owner, the College’s Data Protection Officer and the Compliance and Information Governance Manager:***

1. where sensitive personal data is proposed to be processed as part of the project or activity; and/or
2. where the Information Asset Owner is not able to identify satisfactory solutions to any identified risks or is uncertain as to whether any solutions appropriately address the identified risks; and/or
3. where the project or activity will involve the processing of personal data about 250 or more individuals,

the Information Asset Owner should approve **and then seek a further sign off on the DPIA from the College’s Data Protection Officer and the Compliance and Information Governance Manager**.

**Step 10 - Record keeping**

There should be a permanent record of who signs off any DPIA and when this took place. Accordingly, each Information Asset Owner must:

* retain a copy of the final completed DPIA for his/her records (regardless of whether only the screening questions have been completed or the full DPIA has been completed); and
* send a copy of the final completed DPIA to the local Data Protection Co-Ordinator (if one has been nominated) (regardless of whether only the screening questions have been completed or the full DPIA has been completed); and
* send a copy of the final completed and approved DPIA to the College’s Data Protection Officer (regardless of whether only the screening questions have been completed or the full DPIA has been completed).

If any approval is granted on the basis that certain actions are to be taken by a set deadline and those actions are not completed by that deadline, the project or activity lead should bring this to the attention of the approvers and suggest appropriate remedial action.