DPA CoP 07: Data Protection Impact Assessment

Introduction

1.1 This Code of Practice is to be read in conjunction with the Information Security Policy, Data Protection Policy and wider Information Governance Policy Framework.

1.2 It governs the completion of the Data Protection Impact Assessments (DPIAs), whether it be on an 'as required' basis (within ICT project management methodology or wider business as usual application), or for Information Asset Owners to complete as part of their annual review of their information assets.

1.3 A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.

You must do a DPIA for processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing as explained in Annex 1.

Data Protection Impact Assessment

2.1 DPIAs are made through the creation of Data Activity Risk-assessment Tool (DART) entries and associated Data Set records. DART is the university's online platform which creates DPIAs and populates the Records of Processing Activities as outlined via https://www.imperial.ac.uk/admin-services/secretariat/policies-and-guidance/data-assessments/ which identifies responsible personnel including the Information Asset Owner and Information Asset Administrator.

2.2 Information Asset Owners are required to manage their records in accordance with the responsibilities outlined via https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/college-governance/charters-statutes-ordinances-regulations/policies-regulations-codes-of-practice/information-systems-security/Information-Governance-Policy-Framework.pdf.

2.3 Information Asset Owners should undertake a review of DPIAs at least once a year as part of the Annual Declaration process, and certainly when there is a significant change in the cited activity, the hosting of the activity, or significant legislative or policy changes which impact on the personal data held within.

2.4 Information Asset Owners must ensure that the security of their asset meets the requirements set by the relevant policy accessed via https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/college-governance/charters-statutes-ordinances-regulations/policies-regulations-codes-of-practice/information-systems-security/Information-Security-Policy-v7.0.pdf, which includes:

- All users are properly authorised before they may access the data.

  - Appropriate levels of security are adopted according to the value and/or sensitivity of the data.
  - Must report any incident which results in, or has the potential to result in, a breach of security to the ICT's Service Desk immediately and the Data Protection Team via Data Breach Form.

2.5 A DPIA must be completed if the university plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

2.6 The ICO also state we must always complete a DPIA when / if some specific data processing activities occur, see Annex 1 for full details and examples:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric or genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

2.7 Your DPIA will:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, legality, proportionality and compliance measures;
- identify any external data sharing or use of data processors
- identify any international data transfers, assess the associated risks to individuals then evidence how they will be mitigated.

ANNEX 1 – Examples of High Risk Data Processing.

The follow are examples of 'High Risk' data processing activities as suggested by the Information Commissioners Office (ICO).

Types of Processing which require a DPIA	**Description**	**Non-exhaustive examples of existing areas of application**
Innovative technology	Processing involving the use of new technologies, or the novel application of existing technologies (including AI). A DPIA is required for any intended processing operation(s) involving innovative use of technologies (or applying new technological and/or organisational solutions) when combined with any other criterion from WP248rev01.	• Artificial intelligence, machine learning and deep learning • Connected and autonomous vehicles • Intelligent transport systems • Smart technologies (including wearables) • Market research involving neuro-measurement (i.e. emotional response analysis and brain activity) • Some IoT applications, depending on the specific circumstances of the processing
Denial of service	Decisions about an individual's access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) or involves the processing of special-category data.	• Credit checks • Mortgage or insurance applications • Other pre-check processes related to contracts (i.e. smartphones)
Large scale profiling	Any profiling of individuals on a large scale	• Data processed by Smart Meters or IoT applications • Hardware/software offering fitness/lifestyle monitoring • Social-media networks

		- Application of AI to existing process
Biometric data	Any processing of biometric data for the purpose of uniquely identifying an individual. A DPIA is required for any intended processing operation(s) involving biometric data for the purpose of uniquely identifying an individual, when combined with any other criterion from WP248rev01	- Facial recognition systems - Workplace access systems/identity verification - Access control/identity verification for hardware/applications (including voice recognition/fingerprint/facial recognition)
Genetic data	Any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject. A DPIA is required for any intended processing operation(s) involving genetic data when combined with any other criterion from WP248rev01	- Medical diagnosis - DNA testing - Medical research
Data Matching	Combining, comparing or matching personal data obtained from multiple sources	- Fraud prevention - Direct marketing - Monitoring personal use/uptake of statutory services or benefits - Federated identity assurance services
Invisible processing	Processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or	- List brokering - Direct marketing - Online tracking by third parties - Online advertising

	involve disproportionate effort (as provided by Article 14.5(b). A DPIA is required for any intended processing operation(s) involving where the controller is relying on Article 14.5(b) when combined with any other criterion from WP248rev01	• Data aggregation/data aggregation platforms • Re-use of publicly available data
Tracking	Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment. A DPIA is required for any intended processing operation involving geolocation data when combined with any other criterion from WP248rev01	• Social networks, software applications • Hardware/software offering fitness/lifestyle/health monitoring • IoT devices, applications and platforms • Online advertising • Web and cross-device tracking • Data aggregation / data aggregation platforms • Eye tracking • Data processing at the workplace • Data processing in the context of home and remote working • Processing location data of employees • Loyalty schemes • Tracing services (tele-matching, tele-appending) • Wealth profiling – identification of high net-worth individuals for the purposes of direct marketing
Targeting of / processing data of children / other vulnerable individuals	The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling, data processing or other automated decision-making, or if you intend to offer online services directly to children.	• Connected toys • Social networks • Outreach activities • Research

Risk of physical harm	Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.	• Whistleblowing / complaint procedures • Social care records

Document Control

Document title:		DPA CoP 07: Data Protection Impact Assessment	
Version:	3.1	**Date:**	November 2025
Initially approved by and date:		Provost Board / March 2016	
Version approved by and date:		Data Protection Officer / November 2025	
Version effective from:		November 2025	
Originator:		Division of the University Secretary	
Contact for queries:		Data Protection Officer	
Cross References:		Data Protection Policy - https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/information-governance/Data-Protection-Policy.docx Information Security Policy - https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/college-governance/charters-statutes-ordinances-regulations/policies-regulations-codes-of-practice/information-systems-security/Information-Security-Policy-v7.0.pdf Information Governance Policy Framework - https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/information-governance/Information-Governance-Policy-Framework---to-be-reviewed.pdf	
Notes and latest changes:		March 2016 V0.4 - Draft prepared June 2016 V0.5 - Revised draft to include reference to IAR July 2016 V0.6 - Reviewed by IGSG December 2016 V1.0 - Published online November 2017 V1.1 - Pre-GDPR review undertaken March 2018 V1.2 - Final draft presented to IGSG May 2018 V2.0 - Version published March 2019 V2.1 - Draft reviewed by IGSG / IGOG May 2019 V2.1 - Version published October 2023 2.2 - Removal of references to old IAR. Embedded references to new IAR – DART - Removed reference to wording captured under CoP05 IAR - Removal of APPENDIX which related to old IAR February 2025 V3.0 - Updated to meet new brand standard November 2025 V3.1 - Removed hidden URLs to improve accessibility - Renamed DART	