DPA CoP 08: DPA Considerations for use of Artificial Intelligence (AI)

Introduction

1.1 When AI tools or platforms process personal data or special category data — like names, student IDs, grades, even email content and/or medical / health / biometric information — it falls within scope of data protection legislation. In the UK, data protection legislation is made up of the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) and together, they regulate the collection and use of personal data which is defined as information about identified or identifiable individuals.

1.2 Additionally, administrative law and the Equality Act 2010 are also relevant to providing explanations when using AI, owing to the additional risks they place on unique data types and processing activities which fall within scope of data protection legislation like protected characteristics.

1.3 Whilst presently there is no specific AI legislation within the UK, globally there are numerous legislation and agreements for the university to be aware of, owing to the global footprint which Imperial operates within. Such AI legislation/agreements include;

1.3.1 The Council of Europe Framework Convention on artificial intelligence and human rights, democracy, and the rule of law / https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225;

1.3.2 The European Union Artificial Intelligence Act (EU AI Act) / https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689;

1.3.3 The Indian Digital India Act / http://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf; and

1.3.4 The Chinese AI Safety Governance Framework / https://www.tc260.org.cn/upload/2024-09-09/1725849192841090989.pdf.

Aims

2.1 The introduction of AI based activities and/or integration of AI into current activities, requires the following;

2.1.1 implementation of DPA principles and consideration of data subject rights.

2.1.2 implementation of data protection by design and default

2.1.3 identification, consideration and mitigation of risks caused through the use of AI.

2.1.4 completion of a DPIA and RoPA entry.

2.1.5 identification of any associated documentation and / or current activity that may be affected by its integration.

2.1.6 Engagement with relevant Information Governance and Cyber Security Teams with implementation of new AI based activities not commencing until all actions and reviews have been undertaken.

DPA Principles and rights under data protection legislation relating to AI

3.1 In relation to AI usage, the data protection regulator, the ICO, advises the following four principles are embedded into AI based activities.

3.1.1 be transparent;

3.1.2 be accountable;

3.1.3 consider the context you are operating in; and,

3.1.4 reflect on the impact of your use of AI on the individuals affected, as well as wider society.

3.2 Under data protection legislation, individuals have rights relating to the data held about them. These include:

3.2.1 The right to be informed, where organisations must inform data subjects (those who's information is being used) about any processing activities including;

- the existence of solely automated decision-making. This is where AI makes decisions without any human element involved.
- any meaningful information about the logic involved in the decision making and wider AI setup; and
- the significance and envisaged consequences for the individual of any decisions / practices / outputs from the use of AI.

3.2.2 The right of access, also known as Subject Access, where the following needs to be explained;

- information on the existence of solely automated decision-making (no human element, only AI decisions) where it produces legal or similarly significant effects;
- meaningful information about the logic involved; and
- the significance and envisaged consequences for the individual.

3.2.3 The right to object to such processing (especially in relation to marketing and profiling) plus a right for individuals **to not** have decisions made solely on automated AI decisions; and

3.2.4 In certain circumstances, the rights to have their data rectified, erased or restricted.

3.3 Furthermore, use of AI will trigger a mandatory requirement to undertake a Data Protection Impact Assessment (DPIA), plus, we must ensure all activities are registered in the university Records of Processing Activities (RoPA). Within Imperial, both DPIA's and the RoPA are completed by utilising the Data Activity Risk-assessment Tool (DART) platform / https://www.imperial.ac.uk/admin-services/secretariat/policies-and-guidance/data-assessments/

High-Risk AI Systems

4.1 Within the EU AI Act, Annex III (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689 - anx_III), it defines several user cases/activity types which would be deemed to qualify as 'High-Risk' should AI be utilised, as such these activities are subject to additional obligations and greater scrutiny. These include;
4.1.1 Biometrics;
4.1.2 critical Infrastructure;
4.1.3 education;
4.1.4 employment;
4.1.5 essential services;
4.1.6 law enforcement;
4.1.7 migration; and
4.1.8 justice.

5 How to implement data protection into the design and use of AI

5.1 Under the legislation, Imperial has a general obligation to implement technical controls and organisational measures which show how data protection has been integrated into our processing activities. This process is known as Data protection by design and default and consists of considering data protection and privacy issues throughout the design and implementation process to ensure it is embedded throughout and is key to demonstrating the university's accountbility . To appease these requirements, when AI is being considered the following must be undertaken;

- Integrate appropriate technical and organisational safeguards to protect the rights of data subjects. This includes not feeding AI Systems with personal data unless reviewed and approved by relevant governance leads within the university such ICT, the Data Protection Team and/or Cyber Security Team; and
- Considering how such integration could affect other Policies, Codes of Practice and Ordinances. For example, using AI to review applications (staff or students) will potentially affect all practices and procedures involved in the current application process and require wider discussions with their respective area / division / faculty leads. These would include all literature and transparency information, decision criteria and appeal procedures etc.
- Ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed and used only by those where appropriate. This would include reviewing
    - the data to include only that what is needed,
    - consider use of anonymised data where possible
    - identifying the relevant legal basis relied upon and if based on consent only then ensuring consent is captured fairly.

5.2 Such actions that achieve the above include;

- testing the security of the AI systems to ensure they align to university standards and requirements;

- not allowing testing / training of AI systems to utilise personal data without expressed consent an/or awareness of data subjects;

- adopting a 'privacy-first' approach with any default settings of systems and applications set to minimum;

- ensuring you do not provide an illusory choice to individuals when collecting their data and explaining what it will be used for;

- not processing additional data unless the individual is informed and, where necessary, consent to the processing has been collected;

- testing the AI to minimise bad / flawed data which can lead to biased outcomes;

- have challenge / check points in place to allow for decisions to be reviewed and, where necessary, overturned or corrected;

- ensuring that personal data is not automatically made publicly available to others unless the individual decides to make it so; and

- providing individuals with sufficient controls and options to exercise their data rights.

5.3 There is no one size fits all approach to this so as part of any scoping exercise, planning, creation etc. often will involve the creation of a DPIA which within the university is done by completing a DART entry and allows for the above – and other factors – to be considered and integrated to minimise risk and bake in data protection into all such activities.

5.3.1 To find out more and access DART please see https://www.imperial.ac.uk/admin-services/secretariat/policies-and-guidance/data-assessments/

Documenting AI Activities

6.1 To assist in the understanding, identification and mitigation of risks relating to AI activities, the following is required to be recorded within DART in line with EU legislation:

6.1.1 A general description of the AI system/activity, including:

6.1.1.1 its intended purpose, the name of the provider (supplier / creator of the AI) and the version of the system reflecting its relation to previous versions;

6.1.1.2 how the AI interacts with, or can be used to interact with, hardware or software, including with other AI systems (if applicable), that are not part of the AI system itself;

6.1.1.3 the versions of relevant software or firmware, and any requirements related to version updates;

6.1.1.4 the description of all the forms in which the AI is placed on the market or put into service, such as software packages embedded into hardware, downloads, or application programming interface (API);

6.1.1.5 the description of the hardware on which the AI is intended to run;

6.1.1.6 where the AI is a component of products, photographs or illustrations showing external features, the marking and internal layout of those products;

6.1.1.7 a basic description of the user-interface

6.1.1.8 instructions for use, and a basic description of the user-interface, where applicable;

6.2 A detailed description of the elements of the AI and of the process for its development, including:

6.2.1 the methods and steps performed for the development of the AI system, including, where relevant, recourse to pre-trained systems or tools provided by third parties and how those were used, integrated or modified within the AI Provider (be it a separate supplier or the university if created in-house);

6.2.2 the design specifications of the system, namely the general logic of the AI system and of the algorithms; the key design choices including the rationale and assumptions made, including with regard to persons or groups of persons in respect of who, the system is intended to be used; the main classification choices; what the system is designed to optimise for, and the relevance of the different parameters; the description of the expected output and output quality of the system; the decisions about any possible trade-off made regarding the technical solutions.

6.2.3 the description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing; the computational resources used to develop, train, test and validate the AI;

6.2.4 where relevant, the data requirements in terms of datasheets describing the training methodologies and techniques and the training data sets used, including a general description of these data sets, information about their provenance, scope and main characteristics; how the data was obtained and selected; labelling procedures (e.g. for supervised learning), data cleaning methodologies (e.g. outliers detection);

6.2.5 assessment / description of the human oversight measures in place, including any technical / resource measures needed to interpret the AI outputs;

6.2.6 the validation and testing procedures used, including information about the validation and testing data used and their main characteristics; metrics used to measure accuracy, robustness and compliance with other relevant requirements, as well as potentially discriminatory impacts; test logs and all test reports dated and signed by the responsible persons, including with regard to predetermined changes as referred to under point (f);

6.2.7 the cybersecurity measures put in place, usually captured as part of an ICT Architecture Checklist;

6.3 Detailed information about the monitoring, functioning and control of the AI, in particular with regard to: its capabilities and limitations in performance, including the degrees of accuracy for specific persons or groups of persons on which the system is intended to be used and the overall expected level of accuracy in relation to its intended purpose; the foreseeable unintended outcomes and sources of risks to health and safety, fundamental rights and discrimination in view of the intended purpose of the AI system; the human oversight measures needed, including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the deployers; specifications on input data, as appropriate;

6.4 A description of the appropriateness of the performance metrics for the specific AI;

6.5 A detailed description of the risks and there mitigations which are in place. Such risks will include

6.5.1 Identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI can pose to health, safety or fundamental rights when the high-risk AI is used in accordance with its intended purpose;

6.5.2 the estimation and evaluation of the risks that may emerge when the high-risk AI is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse;

6.5.3 the evaluation of other risks possibly arising, based on the analysis of data gathered from any post-market monitoring, incidents or events;

6.5.4 the adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to point 6.5.1.

6.6 A description of relevant changes made by the provider (supplier / creator of the AI) through its lifecycle;

6.7 Where data pertaining to EU data subjects is processes the creation and retention of a '*EU declaration of conformity*';

6.8 A detailed description of the system in place to evaluate the AI system performance in the post-market phase .

Explaining decisions made by AI

7.1 As referenced already, the UK GDPR includes specific requirements surrounding the use of AI and how AI assisted decisions must be explained / rationalised to those whose data is captured.

7.2 Whilst the output of an AI model varies depending on what type of model is used and what its purpose is. Generally, there are four main types of outputs:

- a prediction (e.g. you will / will not be able to do something);
- a recommendation (e.g. you would like this); or
- a classification (e.g. this email is spam);
- generative content (creates new content in response to a question or action);
- decisions (e.g. from the input it receives, decisions on data can be created).

7.3 In some cases, an AI system can be fully automated when deployed, where the above decisions are made relating to personal data this can be deemed an automated decisions should no human be involved in the process if its output and any action taken as a result (the decision) are implemented without any human involvement or oversight.

7.4 Once the outputs have been defined, where those decisions will have direct consequences towards or involve the use of personal data, the decision recipients (those whose data has been processed) should be able to easily understand how the statistical result has been applied to their particular case. To do the ICO suggests considering the following;

- How you present your explanation depends on the way you make AI-assisted decisions, and on how people might expect you to deliver explanations you make without using AI.
- You can 'layer' your explanation by proactively providing individuals first with the explanations you have prioritised, and making additional explanations available in further layers. This helps to avoid information (or explanation) overload.
- You should think of delivering your explanation as a conversation, rather than a one-way process. People should be able to discuss a decision with a competent human being.
- Providing your explanation at the right time is also important.
- To increase trust and awareness of your use of AI, you can proactively engage with those affected / involved by making information available about how you use AI systems to help you make decisions.

What protocols are in place within the university

8.1 Data Activity Risk-assessment Tool (DART)

- Imperial's DPIA and RoPA platform is available for use in order to help manage and record the planning of your AI based activities. For more information and to begin the process please see the following; https://www.imperial.ac.uk/admin-services/secretariat/policies-and-guidance/data-assessments/

8.2 Data Protection Policy;

- https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/information-governance/Data-Protection-Policy.docx

8.3 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

8.4 DPIA Code of Practice;

- https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/legal-services-office/public/data-protection/DPA-CoP-07---Data-Protection-Impact-Assessment.pdf

8.5 Ethics – for research based activities;

- Research Ethics | Research | Imperial College London

Document Control

Document title:	DPA CoP 08 DPA Considerations for use of Artificial Intelligence (AI)		
Version:	1.0	**Date:**	November 2025
Initially approved by and date:	Data Protection Officer November 2025		
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 / Robert J Scott		
Cross References:	Data Protection Policy Information Security Policy Information Governance Policy Framework		
Notes and latest changes:	June 2025 V1.0 (working draft) - Draft created - Reviewed by ICT / Information Governance / IG Faculty leads. Amendments made		