

DPIA: Self-Assessment Checklist

1. Are you collecting/using the following personal data?

- Yes: Data on religious, ideological, political or trade union views or activities
 - e.g. religious affiliation, party affiliation, joining, membership of or leaving an organisation or association with corresponding contents.
- Yes: Data on health, intimate sphere or racial or ethnic affiliation,
 - e.g. data on patients and insured persons that allow conclusions to be drawn about the physical or mental state of health, data concerning sexual orientation or gender affiliation, data on family secrets and conflicts.
- Yes: Genetic data
 - e.g. DNA profile
- Yes: Biometric data
 - e.g. facial images processed with facial recognition software, fingerprint, iris and retina scans.
- Yes: Data on administrative and criminal prosecutions or sanctions
 - e.g. data on the initiation, conduct and conclusion of prosecutions, data on convictions by criminal justice bodies, data on searches for persons.
- Yes: Data on social assistance measures
 - e.g. information on grants or allowances received.
- No, none of the above

2. Are data of particularly vulnerable persons processed?

- Yes: Minors (< 18 years old)
- Yes: Students
- Yes: Employees
- Yes: Impaired people
- Yes: Patients
- Yes: Mentally ill persons
- Yes: Asylum seekers
- Yes: People on social assistance
- Yes: Elderly people
- No, none of the above

3. Is a decision made automatically that has a legal consequence for the data subject or significantly affects him or her (automated individual decision)?

e.g. projects intending to impose a sanction by means of an algorithm that links the photographed number plates to the suspected vehicle driver by linking them to other data, award of a social benefit by means of an algorithm, provide a tax assessment by means of an algorithm that analyses the data and issues a ruling based on it, evaluate the admission level of a student, automatically grade a student, etc.

 Yes No**4. Are new technologies being used (incl. new artificial intelligence)?**

e.g. use of facial recognition software, application of algorithms for cross-analyses of income and wealth fluctuations to combat social security fraud, application of software programmes for the purpose of making predictions about future offences (predictive policing), use of natural language processing models or software with the aim of offering automated services, collision avoidance software for self-driving vehicles, automated medical diagnostic tools, etc.

 Yes No**5. Is the personal data obtained without the knowledge of the data subject?**

e.g. data scraping on online forums without informing the users, social science projects where it is required not to reveal the true purpose of the project (deception), etc.

 Yes No**6. Does the data processing concern a large amount of data or a large number of persons? Is the data processing extensive in terms of time or geography?**

e.g. processing of a large amount of data from social media users, long-term or permanent video surveillance of a space in real time (with or without data retention), collection of personal from different countries, collection of personal data belonging to more than 10,000 people.

 Yes No**7. Are you matching or combining different datasets?**

e.g. combining an Internet history with other data, combining social media data with other public data, combining different public registers, combining different EPFL-internal databases, etc.

 Yes No**8. Will the personal data be disclosed to industrial third parties (companies) or third-parties located in a country with an insufficient level of data protection in the eyes of the Swiss authorities?**

e.g. Azerbaijan, Georgia, Russia, San Marino, Serbia, Turkey, Ukraine, United States, all Central American countries, all South American countries except Argentina and Uruguay, all African countries, all Asian countries. In case of doubt, please contact the VPA Legal Affairs for this question.

 Yes No

9. Is the personal data processed for the purpose of automatically assessing personal aspects of a natural person (profiling or high-risk profiling)?

e.g. automated evaluation of data for the purpose of assessing the dangerousness of a person, personal analysis of trading and transaction data by FINMA, evaluation of a person's data (GPS data, data on sleep and dietary behaviour) to assess the state of health, evaluation of a (social media) user for the purpose of assessing its polarization profile or online behaviour, other profiling or predicting activities based on aspects concerning the performance at work, the economic situation, health, personal preferences or behaviour.

 Yes No**10. Does the processing of personal data lead to the monitoring of data subjects?**

e.g. tracking a person's online behaviour, systematic surveillance of public areas (railway station concourse, public transport, public buildings), using a GPS application to locate people, etc.

 Yes No**11. Are you considering that your project may cause other serious interference with fundamental rights?** Yes No

If yes, explain briefly why (please use the text box below):