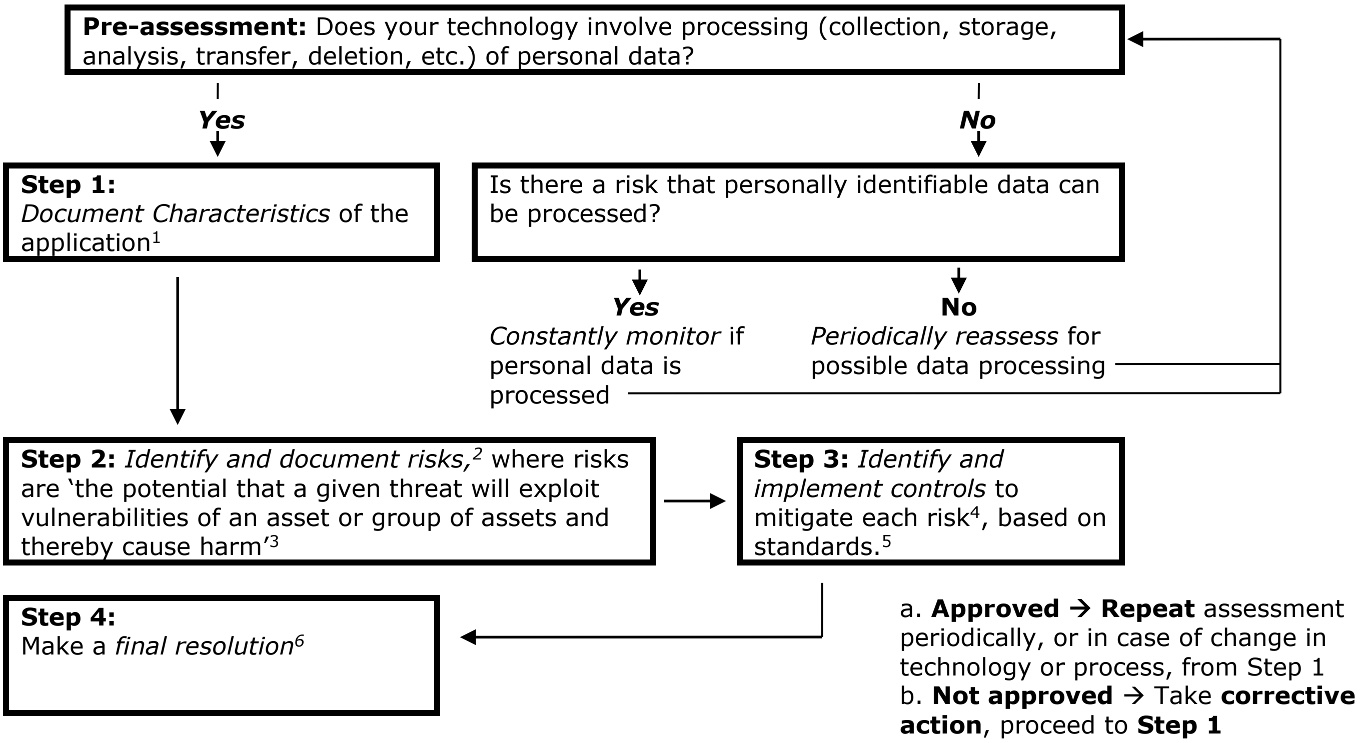
This flowchart was prepared within the Seventh framework project "Future Internet Social and Technological Alignment Research" based on the opinions of Article 29 Working Party (a EU advisory body in the field of data protection)

Data Protection Impact Assessment Flowchart



Pre-assessment: Does your technology involve processing (collection, storage, analysis, transfer, deletion, etc.) of personal data?

Yes

Step 1: *Document Characteristics* of the application[1]

No

Is there a risk that personally identifiable data can be processed?

Yes *Constantly monitor* if personal data is processed

No *Periodically reassess* for possible data processing

Step 2: *Identify and document risks,*[2] where risks are 'the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm'[3]

Step 3: *Identify and implement controls* to mitigate each risk[4], based on standards.[5]

Step 4: Make a *final resolution*[6]

a. **Approved** → **Repeat** assessment periodically, or in case of change in technology or process, from Step 1
b. **Not approved** → Take **corrective action**, proceed to **Step 1**

Compliance with data protection law is an ongoing effort that cannot be ensured by one-time measures. But some strategies, such as Data Protection Impact Assessment ('DPIA'), may facilitate this process. Including DPIA in the development and implementation of your application does not guarantee legal compliance, but may decrease chances of a data protection or data security violations. **This flowchart does not constitute legal advice.**

[1] Including but not limited to: *a comprehensive description of the application, its environment and system boundaries, interfaces with other systems; personal data flows, operation and strategic environment, e.g. stakeholders involved in information collection, the system's mission.*

[2] Namely, *map conditions that may or compromise personal data; consider the significance and likelihood of privacy risks occurring, considering likely uses and misuses of the application, as well as the magnitude of the impact if such risks occur; address the potential impact on a data subject (a patient or other technology user); account for the sensitive nature of the health data processed, and the vulnerabilities of the patients/users whose data is processed; document the outcomes* (among others, to ensure that the process and results of PIA can be audited).

[3] ISO/IEC *27005:2008 definition of risks*

[4] *Namely, analyse measures the technical measures, implemented into the application's architecture ('privacy by design') like default settings, encryption, authentication, etc.; analyse the non-technical measures like management and operational procedures; match each identified risk with a control measure to eliminate or mitigate the risk; Identify residual risks that cannot be addressed by the controls; Document the outcomes.*

[5] E.g. e.g. by ISO/IEC 27001:2013 available at http://www.iso27001security.com/html/27005.html

[6] Assess the trial and the application in the context of its environment and system boundaries*: check if the data protection requirements are met, such as (1) safeguarding quality of personal data; (2) legitimacy of data processing; (3) legitimacy of processing special categories of personal data; (4) compliance with the data subject's right to be informed; (5) compliance with the data subject's right of access to data, correct and erase data; (6) compliance with the data subject's right to object; (7) safeguarding confidentiality and security of processing; (8) compliance with notification requirements, and others.*