

DPIA screening questions

There are two approaches to screening questions: here, I've taken a higher-level approach that will result in more DPIAs than is legally required in the UK, but which will cover processing that is likely to be risky or contentious. The first three on the list are the ones you find in the UK GDPR.

Another approach is to tailor the questions more specifically to what is legally required i.e. attempting to capture the various permutations of the ICO / EDPB pick and mix approach. That's tricky; it will likely result in either loads of questions or a choose-your-own adventure style maze of options. It can be done, but I'm not pretending to have tried it here.

- Are we using to automated / computer-based techniques to profiling or analysing people's behaviour or make significant decisions about them?
- Are we monitoring a publicly accessible place either by CCTV or by monitoring devices?
- Are we using special categories data – e.g. health, sex life, ethnicity, religion, sexuality – about large numbers of people, or more than one type of such data in combination?
- Are we combining data about people from different sources?
- Are we sharing personal data that we hold with new organisations?
- Are we using personal data that we already hold for a new purpose?
- Are we using new technology, especially where that allows us to use or create information about people in a different way than what we normally do now?
- Are we introducing monitoring e.g. location, correspondence, behaviour, or lifestyle, or widening the scope of monitoring we already do?
- Are we using personal data that people would consider to be secret or private?
- Are we using or sharing data about people without their knowledge?
- Are we using data about people who are vulnerable e.g. children, people with physical or mental health conditions, refugees or asylum seekers, or other people who are at risk?
- Are we using information about people in a way that would cause them damage or put them at physical risk if the information is compromised, lost, stolen or accessed by someone not authorised to do so?
- Are we using special categories data or automated techniques to decide whether a person receives a service, interview, job or contract?
- Are we using data about people over whom we have power, or about whom we can make decisions without their consent e.g. employees, tenants or other individual people with whom we have a contractual relationship?
- Are we using biometric data e.g. facial or voice recognition, fingerprints or iris scans?
- Are we using genetic data in a way that identifies people?

If the answer to any of these questions is yes, a DPIA will be helpful, and may be mandatory.