DPIA information gathering crib-sheet (v2.0)

Requirements of GDPR Art 35(7) are in **bold**; requirements for each section (from CNIL, Art29 & ICO) are in *italic.* Comments based on our experiences are in Roman.

**(a) a systematic description of the envisaged processing operations and the purposes of the processing…**

*Data controller and any processors*

*Nature (including new technologies or novel processing), scope, context (number and geographic range of data subjects, our relationship to them, their expectations) , purpose(s) of processing*

*What data are processed*

*How data are collected, stored, processed and destroyed (including retention periods) (identify assets human, technical…)*

*Any other recipients of data*

**… including, where applicable, the legitimate interest pursued by the controller;**

*What’s the legal basis, with justification*

**(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;**

*Data quality and minimisation: adequate, relevant and limited to what is necessary (Article 5(1)(c)); limited storage duration (Article 5(1)(e));*

*Weirdly, no source seems to want an assessment of “proportionality” – i.e. does the purpose justify the processing. But it’s in the GDPR, so think about it here!*

Seems to work to consider individual rights here, too (*ICO confirms this*). According to Art 29s need to look at:

* *information provided to the data subject (Articles 12, 13 and 14);*
* *right of access and to data portability (Articles 15 and 20);*
* *right to rectification and to erasure (Articles 16, 17 and 19);*
* *right to object and to restriction of processing (Article 18, 19 and 21);*
* *relationships with processors (Article 28);*
* *safeguards surrounding international transfer(s) (Chapter V);*
* *prior consultation with DPO (Article 36).*

*And/or, the UK eight principles: fairness, purpose limitation, adequacy, accuracy, retention, rights (see above), security, exports.*

**(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and**

*What impact could the following cause? How likely and severe?*

*Human sources, internal and external, acting deliberately or accidentally*

*Non-human sources: CNIL list malware, epidemics and animals…*

*Resulting in: illegitimate access, unwanted modification or disappearance of personal data*

*In particular, any risks of discrimination, fraud, financial loss, reputational damage, physical harm, loss of confidentiality, reidentification, other significant economic or social disadvantage?*

*See CNIL chapter 3 (pp 10-21) for more details*

We concluded that it was actually easier to think here about \*risks\* arising out of access, modification or disappearance; then look at how those risks might arise from different sources and the mitigations against them in the next section…

**(d) the measures envisaged to address the risks, including safeguards…**

GDPR and regulator guidance is inconsistent on the sub-categories, so collect them first and then work out how they best fit the GDPR wording.

Seemed to work to think of different threat actors here, and work out which mitigations could prevent them causing the risks identified above (including, as recommendations, mitigations we don’t already do). Conclusion needs to state whether there are any risks that \*aren’t\* mitigated down to a level lower than ‘high’.

*Since the GDPR sometimes refers to them as safeguards: contracts or other measures protecting any transfers*

**… security measures …**

*Technical (may include):*

*Logical access control, traceability, monitoring (including of configurations)*

*Anonymisation, pseudonymisation, encryption, data partitioning, reduced retention period*

*Integrity checks, backups, workstation management, malware*

*Secure communications*

*Physical (may include):*

*Location, protection from non-human risk sources (fire, water,…)*

*physical access control*

*security of hardware and paper, both stored and in transmission*

*Organisational (may include):*

*Policy, risk management, project management,*

*Staff management, training, documentation, third parties, maintenance*

*Document marking, archiving*

*Supervision*

*Incident management*

**… and mechanisms to ensure the protection of personal data …**

*audits, logs, etc.* (listed above for now; we can decide how to assign them between security measures and mechanisms later)

**… and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.**

This is now mostly in section (b), so here look at ‘next steps’ – what are we going to do to ensure the DPIA remains valid. E.g. actions to be taken, sign-off, when to repeat the process. And what we need universities, as data controllers to do.