medConfidential early view on ICO sandbox work

A regulatory sandbox, by definition, is only for those with high quality existing practices and a clear and unquestioned governance structure. The data handling practices of data controllers/processors must be unquestionably high for entry to the sandbox.

While lessons must be learnt from experiences of sandbox models in other areas, most notably the Financial Conduct Authority, many of the lessons of 'safe settings' for handling of sensitive data also apply. 'Safe settings' are designed to be robust in the face of inherent risk - normally that is in data identifiability, but in the case of the sandbox, it is around highly increased processing risk with less sensitive data. If there is not higher risk around processing, then the requirements for entry to the sandbox may not be met.

Within the sandbox, "Anonymised" data derived from personal data should be treated identically to personal data about the person from whom it is derived.

All data use in a sandbox should be consensual, safe, and transparent.

1. Consensual

Data subjects have the ability consent/dissent from data use in such environments. If the data controller/processor does not have the capacity to honour such dissents, that should be considered disqualifying under the standards required for access to the sandbox.

2. Safe

Data will be handled only to the highest of standards in a safe setting, not just handled in a 'business as usual' fashion by those who usually find themselves on the receiving end of an ICO investigation.

3. Transparent

Transparency of the proposed sandbox must be at two levels.

> 3a) Systemic transparency: There must be a public register of all projects/organisations applying for entry to the sandbox, what they wish to do, the documents they submit, and the outcomes of their experiments. This follows the existing model for data use by public bodies under the Digital Economy Act 2017 - any public body wishing to use the sandbox would probably have to follow those rules anyway.[1] The same standards must be met by the private sector. If they wish to have obligations under data protection potentially set aside for an experiment, then

[1] E.g. Section 5.1: https://www.gov.uk/government/publications/digital-economy-act-2017-part-5-codes-of-practice/code-of-practice-for-public-authorities-disclosing-information-under-chapters-1-3-and-4-public-service-delivery-debt-and-fraud-of-part-5-of-the-di

they must be transparent about those experiments to avoid the sandbox becoming a toxic dump of inappropriate abuses.

3b) Transparency to data subjects: Data subjects must be able to see how data about them is used, especially as it relates to sandbox activities. While this will rule out some organisations who can not meet the highest standards of data protection principles from the sandbox, if they can not meet the highest standards of data protection, they should not be in the sandbox in the first place. Public bodies are already required to deliver such under point 10 of the Code of Practice on Technology.[2] They must deliver on that requirement if they wish to use the advanced regulatory features of a sandbox.

The ICO must ensure public confidence, and not create an escape route for Data Protection law by the fraudsters and charlatans who will be first in line to play.[3]

medConfidential will reserve judgment on whether the sandbox is a good idea until we see its final form, and the compromises made. We are happy to engage as this process continues.

medConfidential
September 2018
coordinator@medConfidential.org

[2] https://www.gov.uk/guidance/make-better-use-of-data
[3] https://medconfidential.org/wp-content/uploads/2018/04/pharmacy2u-monetary-penalty.pdf