Data sharing code of practice – Comments from CREST Members

CREST. Representing the technical information security industry

Data sharing code of practice - Draft code for consultation

Comments from CREST and CREST Members

- CREST believes that that a penetration test could be deemed as being an exceptional data sharing requirement
- The concept of data sharing is often mistakenly thought to purely relate to data pooling, joint controllers etc and a 'two way' flow of data; can some further explanation be added to the paper to clarify that this issue also relates to 'one way' disclosures of data to other controllers i.e. a disclosure to the police or the purchase of data. This would help make sure it gets to the right audience. It is also helpful in framing the relevance of this document in discussions with other parties in other geos who are not familiar with EU privacy concepts. I understand that if you read all of the document you can find this information but it would be helpful if this was more visible up-front.
- It is noted that the section on acquiring databases etc. only talks about lists and not about the acquisition of data that relates to an individual. It would be helpful if this could be broadened.
- The need for security/governance throughout the data life cycle is not particularly well explained. The security section provides very little detailed information. If the reader needs more information they need to click through three other links. Would it be possible to provide a summary in respect of data sharing that is only one click away.
  There is mention of an information risk assessment but this is not explained and the reader can only find out more if they click the security link in the additional reading and even then I could not find anything prescriptive about how to carry this out.
- Greater clarity over the responsibilities of both the 'data provider' and the 'data consumer' would be helpful (preferably broken down in this way). This could be covered under the accountability principle section and under lawful basis, explaining the requirements that relate to disclosing, receiving and further process data.
- There is limited mention of the exemptions that may apply to the data sharing in particular where it is used for research. Further information on the requirement to notify under this use case would be welcomed. As the research exemption is wide it is of interest to all sectors.
- When the International Transfer section is completed can it cover, at least in general, receiving data from other countries including 'third countries'
- Under the emergency section - whilst staff must be empowered to share data, within clear guidelines, I would suggest that any sharing must be auditable and must be transparent to Management/DPO even if it this transparency is 'after the fact'; This is not made clear.
- The addition of a section on ethics is very welcome. Whilst I accept the topic of ethics and privacy are different it would be helpful to link ethics, where possible, with privacy enforcement as there are links including bias and fairness, excessive processing, secondary processing and transparency.
  One specific point about wording. Pge 28 'make sure that the data they are sharing is accurate, for example by requiring a periodic sampling exercise'. However this requirement may or may not be an issue after the data is shared depending on the use case and this should be reflected in the guidance.

- Data sharing under joint controllership is a valid way to approach security testing. One could see circumstances where a tester may get access to personal data and use this to further the aims of a test. An example in the guidance of where this approach is used is of an organisation providing another organisation with access to personal data on its IT system for a specific research purpose. A clear set of responsibilities should be documented when sharing data under joint controllership.
- However, joint controllership is not the only valid approach, for example one controller could pass the data to another, such as the client providing a testing provider with the data of staff in scope, for the testing provider to make decisions on use of the data for testing, but at that point the testing provider could become a controller with all the responsibilities to the data subjects that entails. Obviously needs careful consideration of the practicality of taking on this responsibility.
- When data sharing is involved between any two organisations, even if the testing provider is a processor only, it is recommend that a DPIA is conducted.