Subject: DPIA Regulations: What to learn from the EU Experience | Odia Kagan
Date: Friday, May 6, 2022 at 11:26:57 AM Pacific Daylight Time
From: Kagan, Odia
To: Regulations

Thank you for the opportunity to speak today. Below is a short recap of comments:

1) Don't reinvent the wheel: Lean on the specificity in the VA and CO laws as a start and on the detailed work that has been done in the EU.

- this is faster to get off the ground and in front of companies looking to comply
- more legal certainty and helpful to multinationals who can leverage EU work they have done.

2) Provide clear, but not too specific guidelines for when a DPIA is needed

As per Brene Brown “Clear is kind, unclear is unkind”

- Provide parameters for when a DPIA would be needed
- Provide a decision tree if possible
- Don't be too specific (For example: EU European Data Protection Board (EDPB) rejected a member state blacklist that required a DPIA just for processing sensitive information or cross border transfer).
- Consider also providing "white list" where a DPIA would not be needed (like EU did).
- Provide guidance on when to revisit the DPIA (eg. technological advances, changes in processing; post M&A acquisition)
- Define the input that service providers can provide to assist the business (Consider issuing guidance encouraging/expecting assistance from the large providers - especially for transparency).
- Provide guidance on how to integrate with other risk assessments

3) Provide clear, but not too complicated, guidelines for how to carry out a DPIA

- Leverage the EU Models: ICO, CNIL (with the taxonomies), NL, ES, DE. and/or ISO 29134 (updated).
- Leverage ISMS and built the Privacy MS on top.
- ICO - very easy to read the model - a lot of leeway but there may be issues with wrong implementation (the proportionality/necessity assessment component is open ended)
- Germany – Very complex and detailed model - that may be a deterrent especially to SME. It does map the TOMs to the risks which can be helpful but there should also be an SME friendly model.
- Provide guidance re: risks to consider: Leverage existing harms and risk taxonomies like Daniel Solove, Jason Cronk, Ryan Calo.
- Provide guidance re: determining probability of occurrence
- Provide guidance on how to carry out the process: for example - 3D model - that requires you to break the processing down into phases (like: storage, use, modification, sharing) and assets (software, hardware, employees, recipients) and for each phase/asset assess the likelihood + severity of an infringement of the relevant data protection principles.
- Provide guidance both on the document itself but also on the process and the relevant stakeholders within the company. and outside (e.g involve the individuals impacted or not or not always)
- Provide options/guidance for SMEs
- Provide /source recommended DPIAs (e.g. in difficult areas like Algorithm impact assessment as discussed by the EU AI Act)
    - This will allow companies to check whether a DPIA was performed ina similar case

- CNIL has a number of sample analyses (e.g IoT)
- DPC Ireland has recommended a few as "gold standard".

Happy to be a resource to the CPPA on this going forward!

Best regards
Odia

Odia Kagan
Partner, Chair of GDPR Compliance and International Privacy
Fox Rothschild LLP
2000 Market St.
20th Floor
Philadelphia, PA 19103-3222
[redacted]
www.foxrothschild.com

From: Regulations <Regulations@cppa.ca.gov>
Sent: May 3, 2022 1:40 PM
To: Regulations <Regulations@cppa.ca.gov>
Subject: [EXT] Agenda and Teleconference Information for May 4-6 Stakeholder Sessions