Comment from Jaap-Henk Hoepman

 # Some 'editorial' comments
- In the executive summary, I would explicitly say that DPbD is a process.
- Also in the executive summary, I would very explicitly say that DPbD also applies to organisational processes
- I would, for self containedness, also include the full text of article 25 at the start of section 2
- bullet 9, section 2.1.1: add business processes as explicit example
- bullet 24 page 8: "At the same time, effective implementation of principles must not necessarily lead to higher costs.": replace must with do

 # Some higher level comments
In 2.1.1. the difference between a measure and a safeguard is not clear.
Bullet 10 says that "Safeguards act as a second tier" (suggesting they are a second line of defence if measures fail); the examples cited concern data subject rights (that can indeed be seen as a second line of defence if the data controller does not comply the principles of data protection), yet intervention in the processing sounds more like a first-line mechanism than a second-line safeguard. Also bullet 11 says "An example of a technical measure or safeguard is pseudonymization of personal data" suggesting there is no difference really.

"Addressing effectiveness" on page 7 does not give much guidance on when something is effective... The fact that something has actual effect does not make it effective. Example: sticking up an umbrella when it rains does have effect, but when I bike it is not effective in the sense that it will not prevent me from getting wet.

Bullet 19 on page 8 seems to be quite strong. I think it is unreasonable to demand that "controllers must have knowledge of and stay up to date on technological advances, how technology can present data protection risks to the processing operation, and how to implement the measures and safeguards that secure effective implementation of the principles and rights of data subjects in face of the technological landscape." If a controller outsources the processing to a data processor, or if it procures a system from a supplier, it seems more reasonable to demand that these processors or suppliers know what they are doing. Moreover, "stay[ing] up to date on technological advances" could be construed to mean that data controllers need to be aware of academic advances in the field; instead I think what they should be aware of is technologies that are available in the market.

In section 3 I worried that perhaps there were too many design elements.
Perhaps they can be grouped in categories of similar elements? And maybe there are even elements missing: purpose limitation could benefit from isolation (a tactic in the separate strategy), while data minimisation (as understood in this text) could also be reached through distribution (i.e processing in end user devices, another tactic in the separate strategy).

 # A meta comment
Reading this I wondered to what extent article 25 creates a requirement for data controllers to go beyond (in terms of designing privacy friendly systems) than what is required in the remainder of the GDPR. Example: if technology A mitigates the risks to the data subject within acceptable ranges, is there any requirement to use technology B instead if it reduces these risks even further. And to what extent is this decision influenced by the costs of using A or B (i.e if B is more expensive, does that make it acceptable to use A instead), or the fact that A really does not reduce the risk to the data subject enough?