Funded by European Union's Rights, Equality and Citizenship Programme (REC)

DPIA

byDesign: Facilitating GDPR compliance for SMEs and promoting Data Protection by Design in ICT products and services

(www.bydesign-project.eu)

DPIA as a GDPR accountability tool and ICT role

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

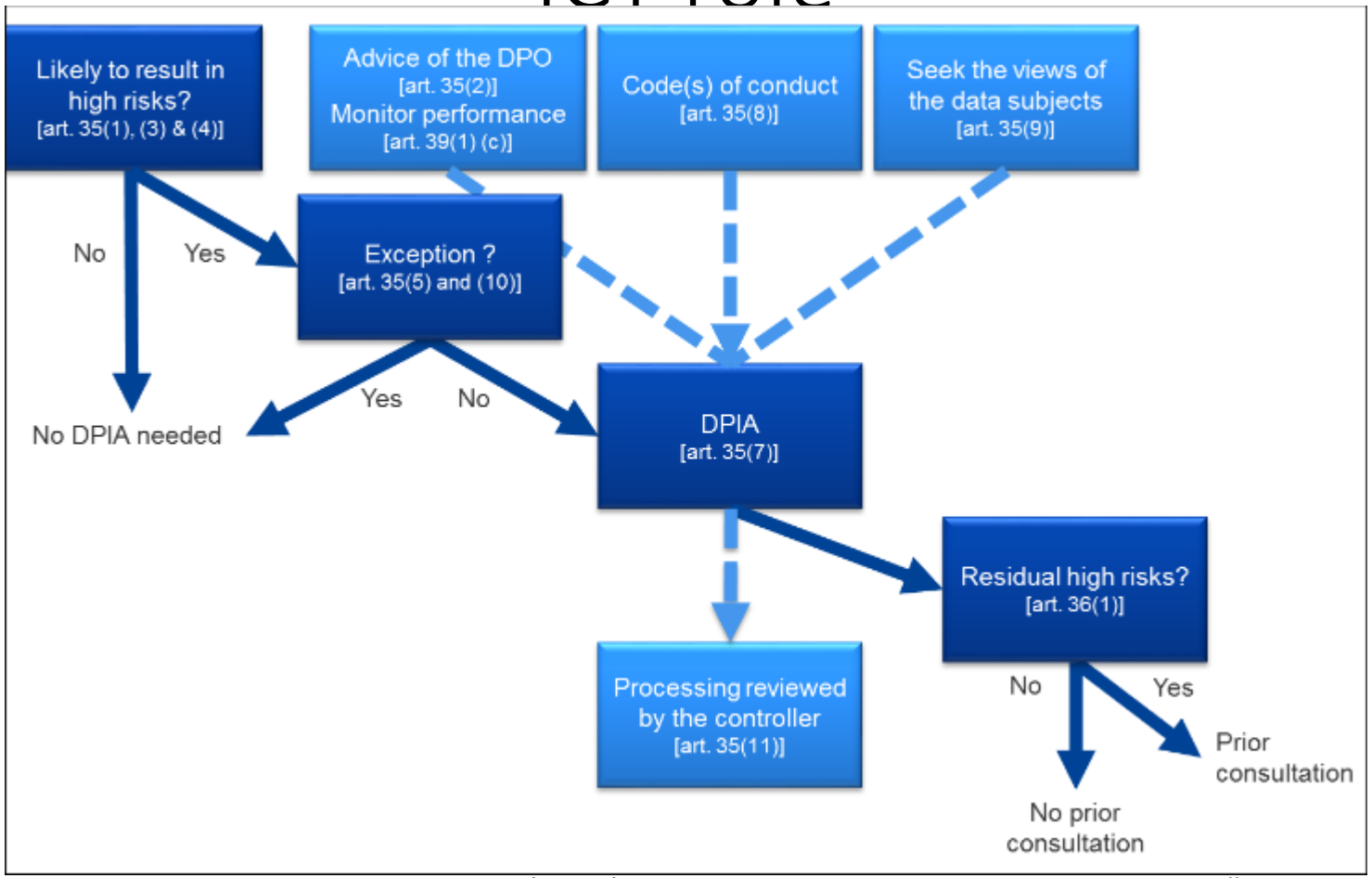
- Accountability Principle intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including supervisory authorities

	Responsible	Accountable	Consulted	Informed
Top Management		X		
Business owner	X			
DPO			X	
IT department			X	
Processors, where relevant			X	
Data subject representatives			(X)	

[Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation, EDPS, 2018]

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

DPIA as a GDPR accountability tool and ICT role



DPIA is further analysed in next seminars…

[Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP29, 2017]

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

DPIA as a GDPR accountability tool and ICT role

	Fairness	Transparency	Purpose limitation	Data minimisation	Accuracy	Storage limitation	Security
Collection	X	X	X	X	X		X
Merging datasets	X	X	X	X	X		X
Organisation/structuring			X	X	X		
Retrieval/consultation/use	X	X	X		X	X	X
Editing/alteration		X		X	X		X
Disclosure/Transfer	X	X	X	X	X		X
Restriction			X	X	X	X	X
Storage	X	X	X			X	X
Erasure/destruction			X			X	X

[Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation, EDPS, 2018]

DPIA as a GDPR accountability tool and ICT role

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity (gross)	Likelihood (gross)	Controls	Severity (residual)	Likelihood (residual)
1	Electronic repository of personal files	Unauthorised secondary use	Purpose limitation, Security	3	3	Staff receive DP training. Access control list limits access to those with need to know. Accesses are logged and logs analysed; see points A, B, C of EUI Security Policy XYZ.	3	1
2	Electronic repository of personal files	Corruption of data	Data quality, security	4	1	Changes are logged and backups kept	1	1
…								
n								

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

Role of the DPO with respect to DPIA and records of processing activities

- What is the role of the DPO with respect to data protection impact assessment?
- The controller should seek the advice of the DPO, on the following issues, amongst others:
  - whether or not to carry out a DPIA
  - what methodology to follow when carrying out a DPIA
  - whether to carry out the DPIA in-house or whether to outsource it
  - what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
  - whether or not the data protection impact assessment has been correctly carried out and
  - whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with data protection requirements

[Guidelines on Data Protection Officers ('DPOs'), WP29, 2017]

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

Thank you for your attention!