Minimizing privacy risks

From the DPO perspective

Prof. Hernan Huwyler

COPENHAGEN COMPLIANCE
Global GRC Solutions

Global Data Protection Day
by Copenhagen Compliance

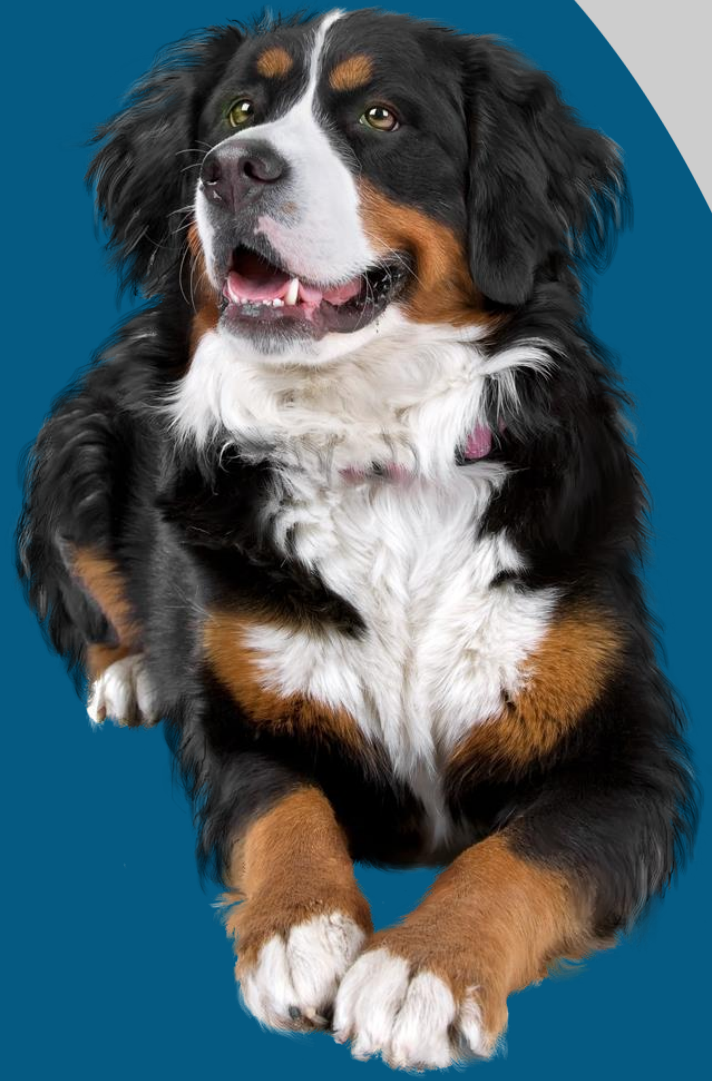
COPENHAGEN COMPLIANCE
Global GRC Solutions

The compliance think tank in the Nordics and beyond

Certifications Compliance Privacy InfoSec Risk

E-Compliance Academy

The unclear ownership of privacy risks is still a major issue for GDPR compliance



E-Compliance Academy

DPO, CISO, CIO, CPO, COO and legal advisors

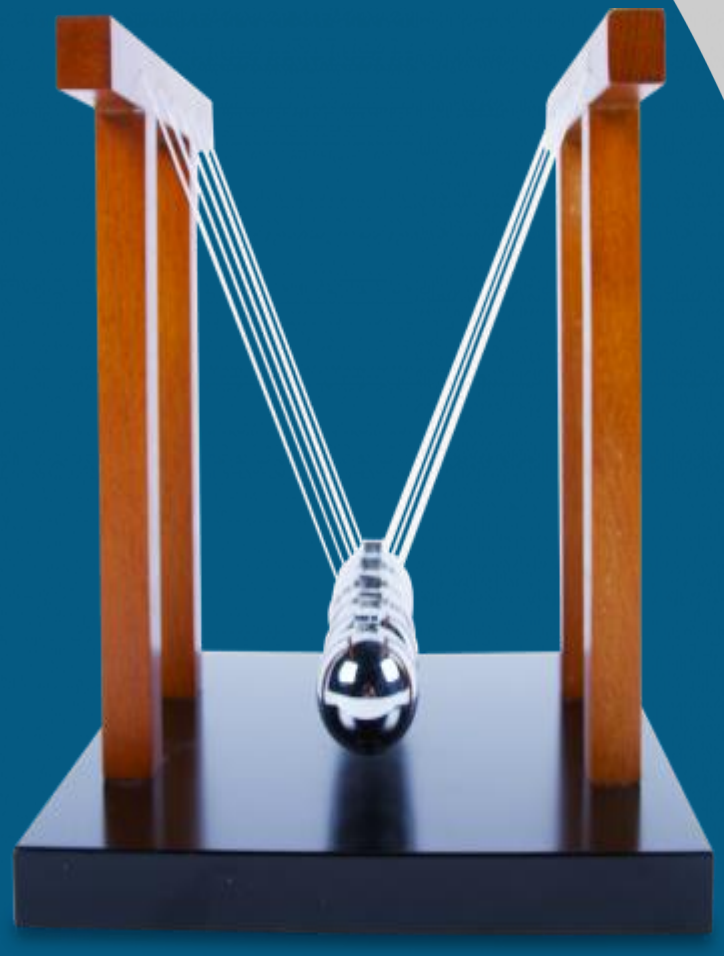
E-Compliance Academy

The roles to control privacy risks become uncoordinated when the GDPR implementation committees ended

Gaps in roles prevent a cost-efficient allocation of resources and creates blind spots

E-Compliance Academy

Unclear internal roles affect the efficiency of instructions, contractual requirements and due diligence of processors



E-Compliance Academy

The CISO monitors the risks on the confidentiality, integrity and availability of personal data

E-Compliance Academy

The DPO monitors the risks on the lack of GDPR compliance triggered by cyber and legal threats

E-Compliance Academy

Policy ownership

CISO	DPO
Security policy	Privacy policy
Acceptable use	Subject requests
Data classification	ROPA inventory
Access control	Consents
Loss prevention	Breach response

E-Compliance Academy

Desperate need for doers able to translate legal requirements into cyber controls, SOPs and technology

E-Compliance Academy

Joint and several liability

Each joined controller is liable for the full GDPR requirements of a contract with the same data subject

E-Compliance Academy

Joint and several liability

All privacy risks are assessed by each joined controller, even for the processing done by the partner

Solution

Flow managers allow modular DPIAs to accelerate the completion

E-Compliance Academy

Solution

Cyber security, business and legal experts complete different risk modules

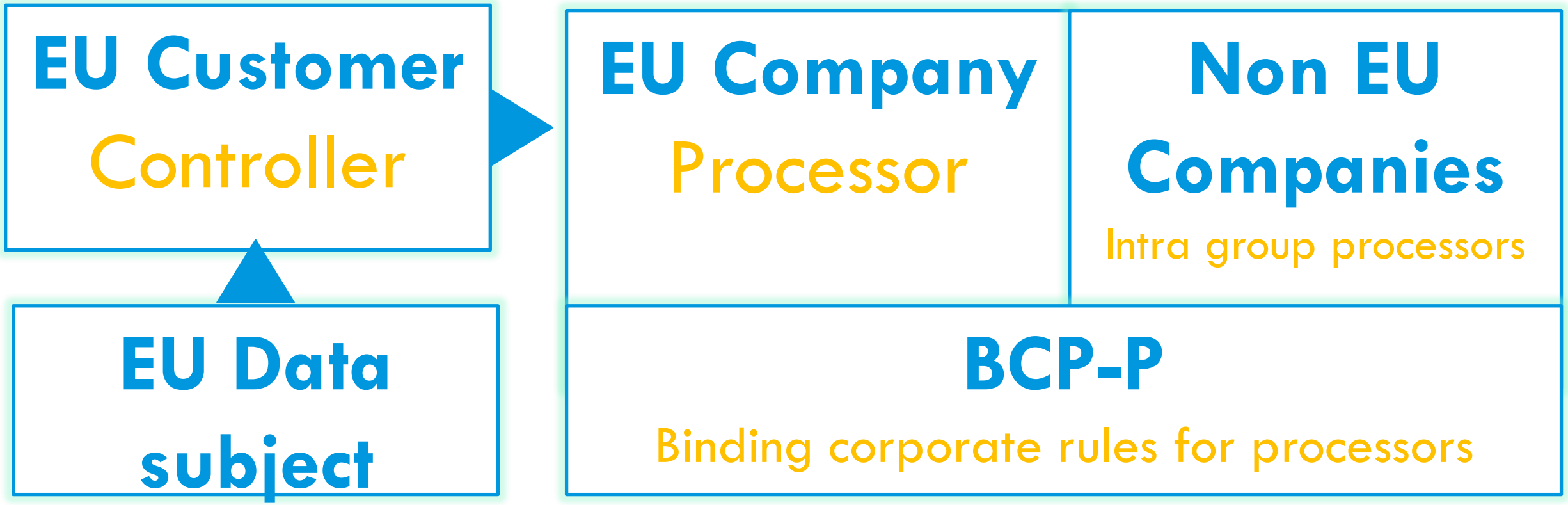
Solution

The approval flows are escalated to the DPO, the CRO and the contract owner

E-Compliance Academy

The binding corporate rules should cover the requirements, transfers and controls of data processing contracts

Transfer scheme



E-Compliance Academy

Non-EU intra-group processors should standardize and coordinate the execution of controls and access requests

E-Compliance Academy

@hewyler

/hernanwyler

mydailyexecutive.blogspot.com

E-Compliance Academy

E-learning platform for Insights/Online Seminars