Data Protection Officer (DPO) Maturity Pathways
a proposal

Based on talks with many DPOs. How do DPOs act and make decisions?

	general description	way of work	use of data
reactive ***case by case***	The DPO knows what to do and focuses on high risk issues, whilst addressing unforeseen cases and answering questions. Responding to incidents.	Getting things done. Learning case by case. Implementing best practices in the field.	Documenting evidence in the GDPR registers. Creates management reports.
reactive ***controlled processes***	The DPO is in control and has standard answers for standard questions and standard procedures for standard issues. Can focus on high risk issues and specific questions. Planning work and responding to incidents.	Responding successfully in an organised manner, following a chosen framework. Providing best practices. Roles and responsibilities are clear and actions have known starting points and predictable outcomes.	Creating dashboards fed by GDPR registers to have a helicopter view which enables zooming in where necessary to all relevant details. Creates monthly tailored reports for various target groups.
pro active ***analytic use of data***	The DPO is in control and has in place a feedback loop from frequently asked questions to role specific training modules. Understands patterns in behaviour within and outside the organisation (suppliers / partners) and root causes of incidents.	Privacy specialists are embedded in projects with possible high risk processing. Specialist knowledge is involved at an early stage of relevant major changes, armed with adequate assessment tooling and a risk mitigation portfolio.	Data is actionable and triggers correct and effective counter measures. Full time access to relevant information, with relevant information and risk assessments. Evidence based actions and learning cycle from the privacy organisation to the broader organisation and partners.
pro active ***predictive use of data***	The organisation is in control and has in place a continuous feedback loop from frequently asked questions to role specific training modules. The organisation understands risks in possible future scenarios in advance, based on the built knowledge base and knowledge of cause and effect.	Adequate privacy knowledge is embedded in the relevant job profiles of the organisation. Staff performs well on quarterly audits. DPO focuses on privacy aspects and data ethics in strategic (AI) work.	Machine learning detects possible high risk scenarios and risk mitigating measures as input for the privacy aware organisation. The DPO uses random checks and audits to better understand underlying dependencies in terms of vulnerabilities. Tailored relevant communication providing relevant context to groups and individuals for future work.

Marlon Domingus
Erasmus University Rotterdam
marlon.domingus@eur.nl
September 2019

Version: September 22 2019