Data Protection Impact Assessment

Owe Langfeldt
& Tereza Struncova

DPO-EDPS meeting
27/10/16

AGENDA

- DPIA in GDPR & the revision of REGULATION 45/2001
- Related work of the ARTICLE 29 WORKING PARTY
- New supervisory architecture
- WAY FORWARD

DPIA – **GDPR & revision of REGULATION 45/2001**

Regulation 45/2001 should be **ADAPTED & APPLIED** in the light of the GDPR & the adaptations should **allow for application at the same time** as GDPR (recital 17), so it provides indications as to the:

→ TIMING: **25 May 2018** (Article 99(2))

→ TRESHOLD: processing operations likely to result in a **HIGH RISK** – when mandatory? (Article 35(1), (3) & 4))

→ METHODOLOGY: what? why? what risks? what can be done about it? (Article 35(7))

also TERMINOLOGY (Article 35(1) & (7))

The EDPS recommended that Article 35 GDPR is copied into the revised Regulation 45/2001.

DPIA under GDPR — **TERMINOLOGY**

Article 35(1) & (7) GDPR (& corresponding provision of the revised Regulation 45/2001):

ASSESSMENT OF THE IMPACT OF THE ENVISAGED PROCESSING OPERATIONS **ON THE PROTECTION OF PERSONAL DATA**

CARRIED OUT BY THE CONTROLLER PRIOR TO THE PROCESSING

WHICH CONTAINS **AN ASSESSMENT OF THE RISKS TO THE RIGHTS & FREEDOMS OF DATA SUBJECTS**

AS WELL AS **MEASURES ENVISAGED TO ADDRESS THESE RISKS**, SUCH AS SAFEGUARDS & SECURITY MEASURES

so, **it is NOT**

- assessment of the impact on anything else than personal data protection, e.g. reputation of the institution or agency,
- Information Security Risk Assessment as such,
- general risk assessment in the context of the accountability exercise

DPIA under GDPR – **TRESHOLD**

Article 35(1), (3) & (4) GDPR (& corresponding provision of the revised Regulation 45/2001)

type of processing in particular USING NEW TECHNOLOGIES
is likely to result in a HIGH RISK to the rights & freedoms of natural persons,
such as in particular:

- processing of SPECIAL CATEGORIES / SENSITIVE DATA **ON A LARGE SCALE**

- **systematic & extensive** EVALUATION **based on automated processing**, including profiling, **on which decisions producing legal effects to the natural person concerned** (...) **are based**;

- **systematic MONITORING of a publicly accessible area ON A LARGE SCALE**

as indicated on the LIST of processing operations for which a DPIA is required established by the DPA

DPIA v. Prior checking – **TRESHOLD comparison**

SPECIFIC RISK	HIGH RISK in particular **using new technologies**
any processing of SPECIAL CATEGORIES / SENSITIVE DATA (only data relating to health, offences & criminal convictions)	processing of SPECIAL CATEGORIES / SENSITIVE DATA **ON A LARGE SCALE** (also data revealing racial & ethnic origin, political opinion, religious or philosophical belief, trade union membership, genetic & biometric data, data concerning sex life & orientation)
any EVALUATION of ability, efficiency & conduct	**systematic & extensive** EVALUATION **based on automated processing**, including profiling, **on which decisions producing legal effects** to the natural person concerned (...) are based
processing allowing for LINKAGES between data processed for different purposes not provided for pursuant to national or EU legislation	**systematic MONITORING of a publicly accessible area ON A LARGE SCALE**
processing for the purpose of excluding individuals from a right, benefit or contract	

DPIA in GDPR – **METHODOLOGY**

Article 35(7) GDPR (& corresponding provision of the revised Regulation 45/2001)

- SYSTEMATIC **DESCRIPTION** OF THE ENVISAGED **PROCESSING OPERATIONS & THE PURPOSES** OF THE PROCESSING,

- ASSESSMENT OF THE **NECESSITY & PROPORTIONALITY** OF THE PROCESSING OPERATIONS IN RELATION TO THE PURPOSES;

- ASSESSMENT OF THE **RISKS TO THE RIGHTS AND FREEDOMS OF DATA SUBJECTS**;

- **MEASURES ENVISAGED TO ADDRESS THE RISKS**, INCLUDING SAFEGUARDS, SECURITY MEASURES AND MECHANISMS TO ENSURE THE PROTECTION OF PERSONAL DATA & TO DEMONSTRATE COMPLIANCE WITH THE GDPR (revised Regulation 45/2001) TAKING INTO ACCOUNT THE RIGHTS & LEGITIMATE INTERESTS OF DATA SUBJECTS OR OTHER PERSONS CONCERNED

DPIA related work of the ARTICLE 29 WORKING PARTY

discussions on the last meetings of the in the Key Provisions & **Technology Subgroups**

→ Questionnaire on DPIA requirements and risky processing operations

→ draft Opinion on DPIA and risks estimated as high in the GDPR
with a list of EXAMPLES OF EXISTING EU DPIA FRAMEWORKS in the annex, i.e.

- Privacy Impact Assessment Guideline, *Bundesamt für Sicherheit in der Informationstechnik (**BSI**)*, 2011,
- *Guía para Evaluación de Impacto en la Protección de Datos Personales (EIPD), Agencia española de protección de datos (**AGPD**)*, 2014,
- Privacy Impact Assessment (PIA*), Commission nationale de l'informatique et des libertés (**CNIL**)*, 2015,
- Code of practice on conducting privacy impact assessments, UK Information Commissioner **(ICO)**, 2014;

- Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by **RFID**,
- WP29 Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications,
- Annex to the WP29 Opinion 9/2001: Privacy and Data Protection Impact Assessment Framework for RFID Applications,
- WP29 Opinion 7/2013 on DPIA Template for **Smart Grid and Smart Metering Systems** prepared by Expert Group 2 Of the Commission's Smart Grid Task Force

DPIA related work of the ARTICLE 29 WORKING PARTY II

on the last meeting of the Technology Subgroup last Thursday, it was announced by the FR rapporteur that

- the objective of this exercise is to identify common requirements and **not to develop one 'European solution' and/or adapt one of the existing DPIA methodologies** listed above (DE, ES, FR or UK),

- the draft Opinion on DPIA & risks estimated as high in the GDPR should be adopted as **DPIA GUIDELINES at the WP29 Plenary in February 2017**,

- some DPIA related legal concepts in the GDPR may already be clarified in the WP 29 DPO Guidelines drafted by the Key Provision Subgroup which should be adopted at the Plenary in November

NEW SUPERVISORY ARCHITECTURE in the GDPR

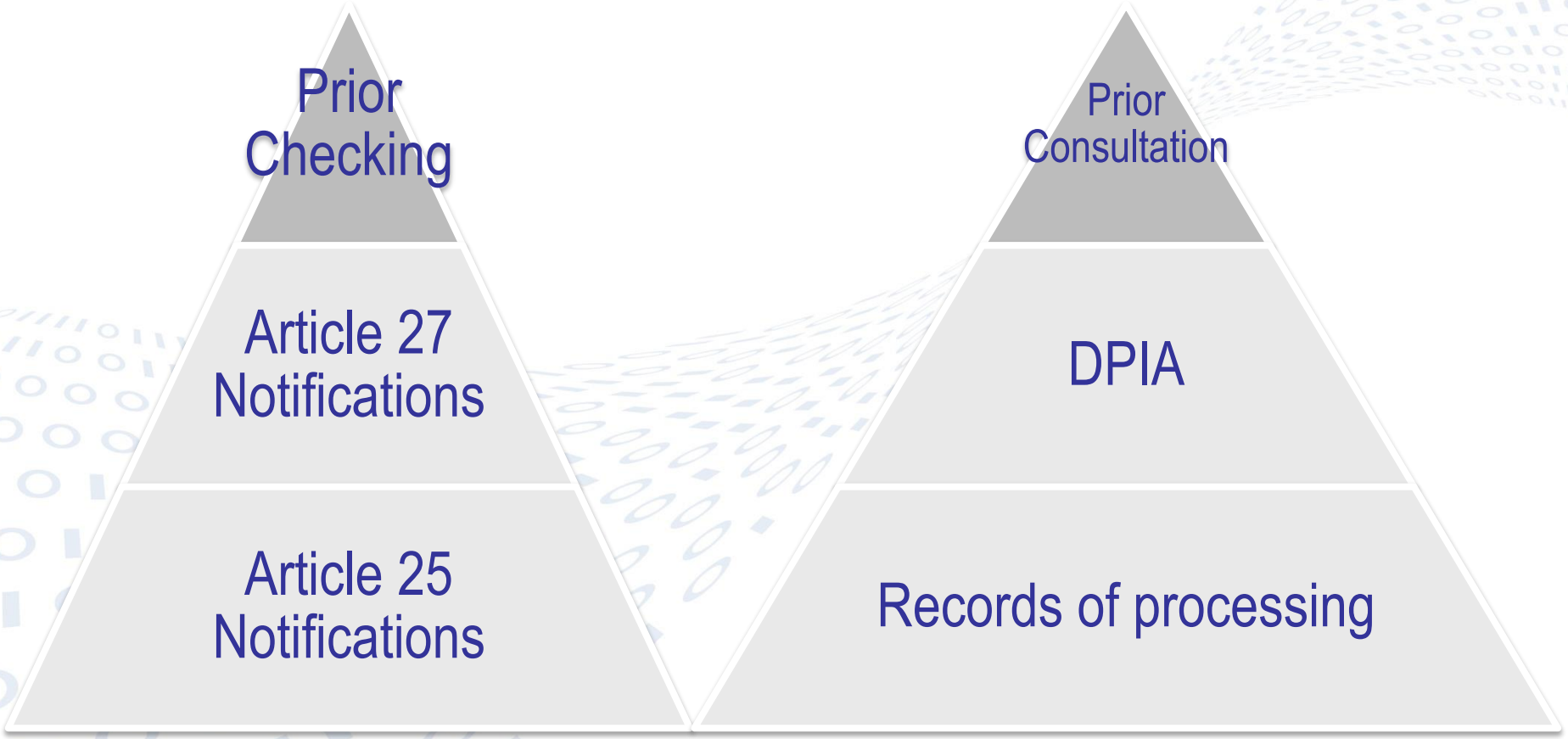
Transition from Articles 25 & 27 notifications and prior checking of processing operations presenting specific risks to obligations

—TO **KEEP RECORDS** of ALL processing activities (Article 30),

—TO CARRY OUT A **DPIA** for processing operations likely to result in a HIGH RISK (Article 35),

—TO SUBMIT the processing operations FOR **PRIOR CONSULTATION** IN THE ABSENCE OF MITIGATING MEASURES (Article 36)

NEW SUPERVISORY ARCHITECTURE - comparison



DPOs INVOLVEMENT in the new architecture

NB - **Article 39 GDPR** & in particular, their tasks

— to inform & advise the controller of their obligations pursuant to the GDPR;

— to provide advice where requested as regards the DPIA and monitor its performance pursuant to Article 35;

— to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter

DPIA – **WAY FORWARD**

- **establish the LIST of processing operations for which the DPIA is MANDATORY** in terms of Article 35(**4**) GDPR (& the corresponding provisions of the revised Regulation 45/2001);

- cooperate with the DPO network to provide the best possible guidance to all interested parties, e.g. organise a case studies based workshop at the next DPO meeting...;

- continue to closely follow the related ongoing work of the Article 29 Working Party;

- continue to closely follow the revision of Regulation 45/2001

NB – timing:

- the draft of the revised Regulation 45/2001 should be presented in January 2017,
- WP29 DPIA Guidelines in February 2017*,
- the next DPO-EDPS meeting should take place in March 2017 in Tallin

- *WP29 DPO Guidelines this November

DPIA – **WAY FORWARD – COOP with the DPO NETWORK**

- How do you see your **role as the DPO** in the DPIA process?
- How do you the **role of the controller** in the DPIA process? How can we help?
- **Which data processing operations do you consider should be subject to DPIA?**
- Should the DPIAs – or its summaries - be **made public**?
- **WHAT SHOULD BE THE NEXT STEPS?**

Thank you for your attention!

For more information:

www.edps.europa.eu

edps@edps.europa.eu

@EU_EDPS

#DPIA #DPO