# Simple now, Complex later

## *The Questionable Efficacy of Diluting GDPR Article 30(5)*

**Harshvardhan J. Pandit**

Email:

*pandithj@tcd.ie*

*me@harshp.com*

*AI Accountability Lab (AIAL), Trinity College Dublin, Dublin, Ireland*

*ADAPT Centre, Dublin, Ireland*

*National Standards Authority Ireland (NSAI)*

*Chair, W3C Data Privacy Vocabularies and Controls Community Group (DPVCG)*

RECITALS

*funding from Horizon Europe research and innovation programme under grant agreement No.101168490 (RECITALS project)

# ~~~ Agenda ~~~

1. EU COM proposal to dilute the GDPR's Article 30
   ***What is the proposal?***

2. Analysis of necessity of Article 30 in GDPR
   ***What will happen because of the dilution?***

3. Alternatives to dilution to achieve same outcomes?
   ***What should be investigated instead?***

# ‘Simplification’

2024

## ‘Better Regulation Agenda’

*EU Commission’s 2024-2029 work program [6]*
*establish competitiveness through “simpler, lighter and faster regulation”*

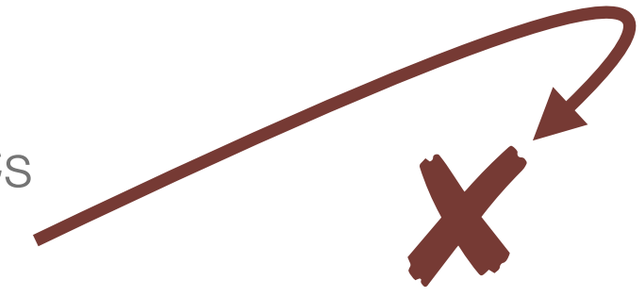
35% reduction in reporting requirements for SMEs/SMCs

Justified through the findings on future of EU competitiveness
— **Draghi report** [12]

2025

Target: “Simplifying rules” reason: GDPR imposes a higher burden on SMEs/SMCs than on larger enterprises; and causes regulatory difficulties

**Proposal to amend the GDPR [16]**
1) extend scope of certifications / codes to SMCs
**2) extend derogations of Art.30(5) to SMCs**



**this is a bad measure!**

now

*Simplification — Digital Omnibus Package*
*(Call for evidence - Ares(2025)7724296)*

What is GDPR Article 30?

What is the principle behind this article?

# What is GDPR Article 30?

GDPR https://eur-lex.europa.eu/eli/reg/2016/679/art_30/oj

*Article 30*

**Records of processing activities**

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

# Proposal to modify GDPR COM(2025) 501 final/2

(1) Increase derogation / exemption scale from 250 employees (SME) to 750 employees (SMC)
(2) Increase exemption scope by requiring “high-risk” instead of “risk” categorisation

*Article 30*

**Records of processing activities**

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 750 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

high risk

# note

## Question:

*If a proposal changes a regulation's obligations such that it affects the implementations regarding rights, should this need an impact assessment?*

## Answer:

*Impact assessments examine whether there is a need for EU action, analyse the possible impacts of available solutions and guide Commission choice and preparation of the proposal. This analysis is carried out during the preparation phase, before the Commission finalises a proposal for a new or revised law.*

*Source:*
*Better Regulation* https://commission.europa.eu/law/law-making-process/better-regulation_en

# Is this proposal creating a ‘better regulation’?

**No Efficacy Established** — **No evidence to understand how, why, where, when, or for whom this will be beneficial.**

**No Impact Assessment** — instead, the proposal notes: “based on experience from implementing legislation. The changes only ensure a more efficient and effective implementation. Their targeted nature and the lack of relevant policy options make an impact assessment not necessary”

**No Scale Assessment** — We DO NOT KNOW how many companies will actually benefit from this proposal.

**No Scope Assessment** — We DO NOT KNOW how many processing activities will meet this exemption

**No Monitoring or Reporting Mechanism** — How will we track whether this proposal has been effective? Do we wait until another 4 years when the periodic GDPR review kicks in?

**No Risks Identified** — How will this affect the enforcement of the GDPR? Were Authorities consulted?

# So will this proposal actually be helpful?

To find out, I utilised an empirical method that evaluates quantity of information and effort for how organisations maintain the Article 30 records, and then to check whether the proposal helps provide an *effective* 35% reduction in documentation.

***Spoiler alert: It does not provide benefits in reality, but instead creates more risks for organisations and authorities, and also for data subjects regarding their rights by extension.***

# What's in a ROPA? — Static Fields

Fields that refer to the organisation's information don't need to be repeated in every ROPA entry and can be specified only once.

Therefore, we refer to them as "static fields".

You declare them once in a document.

| ID | Clause | Information |
|---|---|---|
| **Controller ROPA** | | |
| Static fields – these rarely change | | |
| C1 | 30-1a | Controller name |
| C2 | 30-1a | Controller contact |
| C3 | 30-1a | Joint Controller name |
| C4 | 30-1a | Joint Controller contact |
| C5 | 30-1a | Controller representative name |
| C6 | 30-1a | Controller representative contact |
| C7 | 30-1a | DPO name |
| C8 | 30-1a | DPO contact |

***Burden to maintain: none*** → ***Information also needed in notices and contracts***

# What's in a ROPA? — *Dynamic* Fields

Fields that refer to the '*processing*' must be declared for each *unique* activity. Therefore, we refer to them as "dynamic fields". These form the bulk of the ROPA

| ID | Clause | Information |
|---|---|---|
| **Controller ROPA** | | |
| Dynamic fields – these are per processing activity | | |
| C9 | 30-1b | Purposes of processing |
| C10 | 30-1c | Categories of data subject |
| C11 | 30-1c | Categories of personal data |
| C12 | 30-1d | Categories of recipients |
| C13 | 30-1e | If data is transferred to a third country or international organisation |
| C14 | 30-1e | Third Country or International Organisation as Recipient |
| C15 | 30-1e | Legal Basis for transfer |
| C16 | 30-1e | Safeguards for transfer if legal basis is from Art.49-1 |
| C17 | 30-1f | Time limits for erasure of data categories |
| C18 | 30-1g | Technical and organisational safeguards (e.g., security) |

***Burden to maintain: ???*** → ***Info. needed in ???***

# Exemptions to keep a ROPA

| Burden | Criteria |
|---|---|
| *Low* | E1 – Size of organisation is less than 250 people |
| ***High*** | **E2 – Risk to rights and freedoms has low likelihood*** |
| *Low* | E3 – Processing is occasional |
| *Low* | E4 – Processing does not include Special categories of personal data |

***Information needed to assess risks as per GDPR Article 35 (1) (DPIA)***

| ID | Information |
|---|---|
| C9 | Purposes of processing |
| C10 | Categories of data subject |
| C11 | Categories of personal data |
| C12 | Categories of recipients |
| C13 | Transfer to third country or international organisation |
| C14 | Transfer Recipient |
| C15 | Legal Basis for transfer |
| C16 | Article 49(1) safeguards for transfer |
| C17 | Time limits for data erasure |
| C18 | Technical and organisational measures |

# What's in a ROPA? — *Dynamic* Fields

Support or paradox: To be exempt from documenting some information, you must first have that information at hand to check if the exemption applies…

***Information in a ROPA***

| ID | Clause | Information |
|---|---|---|
| **Controller ROPA** | | |
| Dynamic fields – these are per processing activity | | |
| C9 | 30-1b | Purposes of processing |
| C10 | 30-1c | Categories of data subject |
| C11 | 30-1c | Categories of personal data |
| C12 | 30-1d | Categories of recipients |
| C13 | 30-1e | If data is transferred to a th |
| C14 | 30-1e | Third Country or Internatio |
| C15 | 30-1e | Legal Basis for transfer |
| C16 | 30-1e | Safeguards for transfer if le |
| C17 | 30-1f | Time limits for erasure of data categories |
| C18 | 30-1g | Technical and organisational safeguards (e.g., security) |

***to determine risk-based exemption***

| ID | Information |
|---|---|
| C9 | Purposes of processing |
| C10 | Categories of data subject |
| C11 | Categories of personal data |
| C12 | Categories of recipients |
| C13 | Transfer to third country or international organisation |
| C14 | Transfer Recipient |
| C15 | Legal Basis for transfer |
| C16 | Article 49(1) safeguards for transfer |
| C17 | Time limits for data erasure |
| C18 | Technical and organisational measures |

***You don't have to document it, but you must still maintain it!***

# What happens if ROPA obligation is exempted?

Let's assume you somehow magically know that you don't need to maintain a ROPA because an activity is low-risk
- maybe the Authority guidelines state this
- maybe your experience has taught you this
- maybe you just feel it doesn't as a gut feeling

***What % of effort are you saving by not keeping that information in a ROPA?***

To know this, we must <u>check whether the information in a ROPA is also required in another obligation</u>. If it is, then it must be either:

1) The obligation is satisfied using a ROPA, and **without a ROPA, the effort for that obligation will increase**; OR

2) The ROPA information was generated after that obligation, which means **the information must still be kept for that obligation** even if it isn't maintained in a ROPA

# Impacts on Rights

***ROPA information has a significant overlap with Rights-related information***

| | | principles | transparency | | | rectify | erase | restrict | | portability | objection | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ID** | **Information** | **A5** | **A13** | **A14** | **A15** | **A16** | **A17** | **A18** | **A19** | **A20** | **A21** | **A22** |
| C1–8 | Controller Identity | 5-1a, 5-2 | 13-1a, 13-1b | 14-1a, 14-1b | | | | | | | | |
| C9 | Purposes | 5-1a, 5-1b | 13-1c | 14-1c | 15-1a | 16 | 17-1a | | | | 21-1–3, 21-6 | 22-1 |
| C10 | Data Subjects | 5-1a | | | | | | | | | | 22-1 |
| C11 | Personal Data | 5-1a, 5-1c | 13 | 14-1d | 15-1b | | 17-1a | | | 20-1 | | |
| C12 | Recipients | 5-1a | 13-1e | 14-1e | 15-1c | | | 18 | 19 | | | |
| C13 | Data Transfer | 5-1f | 13-1f | 14-1f | 15-2 | | | | | | | |
| C14 | Transfer Recipient | 5-1f | 13-1f | 14-1f | 15-2 | | | | 19 | | | |
| C15 | Transfer Legal Basis | 5-1f | 13-1f | 14-1f | 15-2 | | | | | | | |
| C16 | Transfer Safeguard | 5-1f | 13-1f | 14-1f | 15-2 | | | | | | | |
| C17 | Erasure limits | 5-1a, 5-1e | 13-2a | 14-2a | 15-1d | | 17-1e | 18-1b | | | | |
| C18 | Tech/Org safeguards | 5-1d, 5-1f | | | | | | | | | | 22-3 |

*This means either:*
*1) Without a ROPA, the implementation of rights will suffer; OR*
*2) Without a ROPA, that information must still be documented for rights*

*Net benefit: Negligible at best*
***Potential Impact: Significant***

# Impact on Obligations

***ROPA information also has an overlap with key GDPR obligations***

| | | DP-by-design | responsibility | security / data breach | | | DPIA |
|---|---|---|---|---|---|---|---|
| **ID** | **Information** | **A25** | **A26** | **A32** | **A33** | **A34** | **A35** |
| C1–8 | Controller Identity | | A26-1 | | A33-1b | A34-2 | A35-1, A35-7a, A35-7b |
| C9 | Purposes | A25-1, A25-2 | A26-1 | A32-1 | | | A35-1, A35-7a |
| C10 | Data Subjects | A25-1 | A26-1 | A32-1 | A33-1a | A34-2 | A35-1, A35-7a |
| C11 | Personal Data | A25-1, A25-2 | A26-1 | A32-1 | A33-1a | A34-2 | A35-1 |
| C12 | Recipients | | A26-1 | A32-1 | | | A35-1 |
| C13 | Data Transfer | | | A32-1 | | | A35-1 |
| C14 | Transfer Recipient | | | A32-1 | | | A35-1 |
| C15 | Transfer Legal Basis | | | A32-1 | | | A35-1 |
| C16 | Transfer Safeguard | | | A32-1 | | | A35-1 |
| C17 | Erasure limits | A25-2 | A26-1 | | | | |
| C18 | Tech/Org safeguards | A25-1, A25-2 | A26-1 | | A33-1d, A33-5 | A34-2, A34-3a | A35-7d |

*This means either:*
*1) Without a ROPA, the implementation of security/data breach/DPIA will suffer; OR*
*2) Without a ROPA, that information must still be documented for these obligations*

*Net benefit: Negligible at best*
***Potential Impact: Significant***

# Note

To date, only 1 fine solely regarding ROPA. All other fines are for ROPA + other obligations.

**Issues in a ROPA are symptoms of other underlying and manifested problems**. By identifying information as being missing, incorrect, or incomplete, the ROPA is a key indicator that it is highly likely there is also something wrong with the other obligations.

# Position of EDPS / EDPB / DPAs

1. "preliminary support" for the proposal under the EDPB and as a joint letter with the EDPS [13, 17]

2. EDPS notes that the proposal does not affect the core principles of the GDPR —> findings show the significant impact on accountability principle

3. EDPB chair asks to ensure proposal would not affect the obligation of controllers and processors to comply with other GDPR obligations —> findings show it does have significant impact on ability to comply

**EDPS, EDPB, and DPAs should revise their positions on the validity of the proposal based on these findings**

# note

the Commission's current proposal to dilute the GDPR should be revised due to its lack of practical usefulness and the high probability that it encourages practices that risk liability and compliance for the organisations it intends to support and promote.

There has been no impact assessment conducted regarding validity of measures, and further – and most importantly – I question whether it will actually lead to the intended outcomes based on the presented analysis.

# Potential Alternatives

**5.1 Distinguish Personal Data Processing as a Business Model**

- Some companies only process personal data because of HR, contracts, legal obligations, etc.
- Other companies run a business with a focus on processing personal data.

5.2 Ensuring Compliance Solutions Are Compliant

5.3 Harmonise Compliance Measures

5.4 Utilise RegTech and eGov Technologies

# Potential Alternatives

5.1 Distinguish Personal Data Processing as a Business Model

**5.2 Ensuring Compliance Solutions Are Compliant**

- Tools used by SMEs/SMCs for compliance (e.g. CMPs) are themselves creating additional liability through non-compliance
- Certification for GDPR compliance provider (*lessons from AI Act's product assurance model*)

5.3 Harmonise Compliance Measures

5.4 Utilise RegTech and eGov Technologies

# Potential Alternatives

5.1 Distinguish Personal Data Processing as a Business Model

5.2 Ensuring Compliance Solutions Are Compliant

**5.3 Harmonise Compliance Measures**

- if SMEs/SMCs find GDPR difficult, its 10x greater for the AI Act due to lack of harmonisation of laws

- Our work [33] shows fragmentation in DPIA requirements and that DPIAs are needed in Annex III AI Act in most cases. So how to do DPIA + FRIA?

5.4 Utilise RegTech and eGov Technologies

# Potential Alternatives

5.1 Distinguish Personal Data Processing as a Business Model

5.2 Ensuring Compliance Solutions Are Compliant

5.3 Harmonise Compliance Measures

## 5.4 Utilise RegTech and eGov Technologies

- Reintroduce ROPA notification system from DPD
- Example from Jamaican DPA
- Common budgeting and resources

# Work on Supporting ROPA


## ISO/IEC TS 27560:2023

Privacy technologies — Consent record information structure

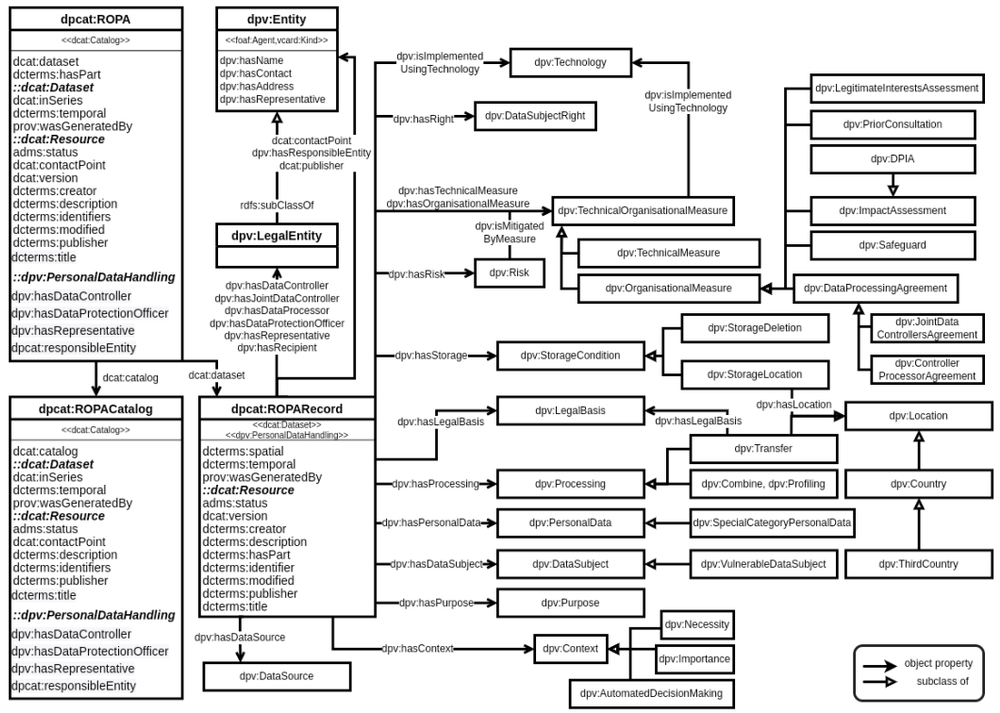
**Published** (Edition 1, 2023)

**Information technologies — Structure of Personally Identifiable Information (PII) Processing Records**

**Revision of ISO/IEC 27560**
**based on GDPR Art.30 analysis of ~30 DPAs resources to support ROPA and the implementation of transparency rights through issuing of a "Privacy Receipt"**

**Guide for using the Data Privacy Vocabulary**
for GDPR's ROPA — supporting ROPA in a machine-readable form in an open specification ;
analysis of how this is necessary for data spaces ;

More work on Health Data Spaces, eIDAS/EUDI wallets, NIS2 incident reporting, and recording AI Act information in same document as an "AI ROPA"



Paper is Open Access
https://doi.org/10.1007/978-3-032-07574-1_6

# dankeschön! / thank you!

Simple now, Complex later
The Questionable Efficacy of Diluting GDPR Article 30(5)

Harshvardhan J. Pandit
pandithj@tcd.ie
me@harshp.com

More work on AI and Accountability at https://aial.ie/

Check out Data Privacy Vocabulary (DPV) https://dpvcg.org/
W3C DPVCG is an open community group - we welcome you!

*Download this presentation at https://harshp.com/research*