UNIVERSITEIT GENT

Third Round of Delphi Study

Start of Block: Welcome Section

Welcome to Delphi Round 3

In this round, we would like to review the remaining PTPs that did not get consensus for inclusion or exclusion in Round 2. In addition, we would like your opinion on changes to the DPIA required for the PTPs for which there was/is consensus regarding their relevance to Big Data Analytics and are important to address in the application of the DPIA to Big Data Analytics.

As described in our analysis in the Round 2 feedback report, we came up with four distinct conditions based on which we defined three consensus types: **Strong consensus**, when all four conditions are met **Almost strong consensus**, when a single condition is not met **No consensus**, when more than one condition is not met
For additional information including our analysis reports, please visit our website, where we post regular updates about our research to all participants. The password for the protected pages is "delphi2022"

If you have questions regarding our survey, you can post them on our website. If you believe any of the questions need further clarification, please let us know.

For any question, please feel free to contact me at: georgios.georgiadis@ugent.be
Important notice: The hyperlinks will open a new window in your browser. This is to prevent you from losing your session on this website, which can result in having to repeat the survey. We apologise for any inconvenience this may cause.

We appreciate your support and understanding and look forward to getting your feedback.

End of Block: Welcome Section

UNIVERSITEIT GENT

Start of Block: Privacy touchpoints

PTPs level of Agreement

We have reached consensus on all the PTPs, except for PTP (6) and PTP (8). We have therefore decided to disregard PTP (8), as it failed all four conditions, both in terms of agreement and importance. As a reminder, PTP (8) refers to problems that come from the DPIA's vague descriptions.

In terms of level of agreement, the feedback received suggests that the templates and methods we already have are good enough. Some of you indicated that the real issue is the low level of engagement of some DPAs due to a lack of expertise in Big Data Analytics - an interesting point that relates to PTP (7) in terms of the limited level of stakeholder engagement.

Importantly, we'd like to know if you would be willing to change your mind on PTP (6), which is about the way to handle different types of risks to privacy and data protection breaches in the DPIA. This PTP has gained consensus for its importance, but not for whether it should be included in the DPIA. Many of you have argued that legal issues and the improper use of technology could lead to privacy and data protection risks, while some have said that these risks don't exist, which is slightly contradictory. **May we ask you to consider these opposing opinions when expressing for the final time your level of (dis)agreement with the following statement?**

PTP (6) Improper treatment of different types of privacy risks and data breaches

Please indicate to what extent you agree that Big Data Analytics solutions could lead to different types of privacy risks and data protection breaches

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree

UNIVERSITEIT GENT

Please give some information on why you agree or disagree with the above statement.

_____

_____

_____

_____

_____

PTPs Level of Importance

Similar to the level of agreement, we have reached consensus on all the PTPs, except for PTP (7) and PTP (8). As mentioned, we will disregard PTP (8) as it failed in all four conditions.

For PTP (7), we would like to ask you again for your revised input, as the feedback we have received from you indicates that their inclusion in the DPIA is actually beneficial, especially for the early detection of possible data processing violations, and should be defined in terms of representation and knowledge, as well as the data to be processed. For that reason, the formulation of the question has been slightly modified but leaving untouched the options introduced in the previous round.

For the same question, we ask you to provide us with an explanation of your reasoning and if possible the list of stakeholder roles that can be representative for assessing the PTPs in the DPIA

PTP (7) Limited range of stakeholders' involvement

Please indicate to what extent you consider it important to include in the DPIA external (to the organization) stakeholders whose data is predominantly processed in a Big Data Analytics application and who need to be identified in terms of data representation and knowledge including data that to be processed.

	○ Very Important	○ Fairy Important	○ Important	○ Slightly Important	○ Not at all Important

Please give some information about the roles or positions of these stakeholders and explain why you agree or disagree with the above statement

_____

_____

_____

_____

_____

End of Block: Privacy touchpoints

UNIVERSITEIT GENT

Start of Block: DPIA Improvements

Proposed Improvements to the DPIA

In the following section, we present our proposals to improve the DPIA, so that it is better aligned with the PTPs agreed in Rounds 1 and 2. We use the Data Protection Impact Assessment (DPIA) rev. 01 Guidelines, adopted on 4 April 2017 and last revised on 4 October 2017, as a reference. To determine the improvements, we have considered your feedback on the prioritisation of DPIA components (see Round 2 feedback report). For your convenience, the four essential components were Guidelines (17%), Knolwedge Base (33%), Method (33%) and Templates (17%).

While there is no single correct answer, we would want to know if you agree with our proposed solution and get your opinion in the following questions. **It is essential to have your input or any of your suggestions regarding how to approach or handle the stated problem.**

Click here to go to the page with copies of the references

PTP (1) Unclear data controllership

Problem: The transfer of big data from one place or recipient to another, results in a diverse controllership. Consequently, it is difficult to understand and ensure compliance with privacy requirements among data controllers. Existing mechanisms that rely on privacy by policy – such as (informed and explicit) consent and privacy notices or 'notice-and-consent' models fail to provide transparency and control sufficient for individuals to understand how their data have been collected and used.

Solution: We propose to expand the 05/2020 guidelines on consent under Regulation (EU) 2016/679 v1.1, adopted on 4 May 2020 and ISO/IEC 29184: 2020, by further developing the idea of the tiered–layered and staged consent model (see [1]). This would improve the comprehension and comprehensiveness of the consent for Big Data operations. To address the complexity of managing this type of consent, a new consensus template or consent management platform as a software support tool might be required.

[1] Bunnik, E. M., Janssens, A. C. J. W., & Schermer, M. H. N. (2013). A tiered-layered-staged

model for informed consent in personal genome testing. European Journal of Human Genetics, 21(6), 596–601. https://doi.org/10.1038/ejhg.2012.237

- ○ Strongly Agree
- ○ Agree
- ○ Undecided
- ○ Disagree
- ○ Strongly Disagree

Please explain your answer and provide any additional suggestions you may have.

_____

_____

_____

_____

_____

PTP (2) Identification of individuals from derived data

Problem: Big Data Analytics techniques enable inferences from undisclosed information that can be used to identify an individual, whether alone or combined with other information. Such features have made re-identification easier – arguably to the point of undermining the value of anonymisation.

Solution: A revised version of the DPIA guidelines should include references to frameworks such as ISO /IEC 27559:2022 that govern the appropriate use of data de-identification procedures. Such a framework for de-identification should be used at all stages of the data

lifecycle, from the development of the means for data collection to internal re-use, across making data available to external partners, to archiving. This should apply to all types and sizes of organisation, including public and private companies, and governmental and not-for-profit organisations. As there is a risk that some techniques could be reverted in the future, the guidelines could indicate a privacy risk assessment to be carried out periodically or under certain conditions, e.g., when the data processing involves more advanced types of analytics techniques.

- ○ Strongly Agree
- ○ Agree
- ○ Undecided
- ○ Disagree
- ○ Strongly Disagree

Please explain your answer and provide any additional suggestions you may have.

_____

_____

_____

_____

_____

PTP (3) Discrimination issues affecting moral or material personal matters

Problem: The increasing risk of statistical discrimination or ‘data determinism’ a by-product of Big Data Analytics, may cause non-material damage to data subjects in accordance with Recital 75 of the GDPR

Solution: The DPIA guidelines should suggest an assessment of the impact of Big Data Analytics algorithms. The objective is to assess the magnitude of any disproportionately negative impact on a protected class and examine whether the algorithm could be replaced with one equally effective but with a smaller disparate impact [1]. Examples of existing frameworks that could assist in this type of assessment are: Fundamental Rights and Algorithm Impact Assessment 'FRAIA' [2] and Fair, Accountable and Transparent 'FAT Flow' [3].

[1] MacCarthy, M. (2018). Standards of Fairness for Disparate Impact Assessment of Big Data Algorithms. SSRN Electronic Journal, 48, 67–148. https://doi.org/10.2139/ssrn.3154788

[2] Government of the Netherlands. (2022). Impact Assessment fundamental rights and algorithms. https://www.government.nl/documents/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms

[3] Martens, D. (2020). FAT Flow: A Data Science Ethics Framework

- ○ Strongly Agree
- ○ Agree
- ○ Undecided
- ○ Disagree
- ○ Strongly Disagree

Please explain your answer and provide any additional suggestions you may have.

_____

_____

_____

_____

_____

UNIVERSITEIT GENT

PTP (4) Lack of transparency

Problem: The opacity of contemporary data processing activities, along with how big data are eventually used, may have nothing to do with the purpose set or anticipated at the time of initial data collection. This could lead to transparency infringements as it increases the risk that data subjects will be unable to assess and exercise their rights

Solution: Similar to PTP (3), the DPIA guidelines should suggest an assessment of the impact of Big Data Analytics algorithms. The Fundamental Rights and Algorithm Impact Assessment 'FRAIA' [1] and Fair, Accountable and Transparent 'FAT Flow' [2]. The latter specifically examines the level of transparency according to the different target entities to whom transparency is offered, such as the manager of the organisation, the data analyst, the model applicant and data subjects.

[1] Government of the Netherlands. (2022). Impact Assessment fundamental rights and algorithms. https://www.government.nl/documents/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms [3] Martens, D. (2020). FAT Flow: A Data Science Ethics Framework

[2] Martens, D. (2020). FAT Flow: A Data Science Ethics Framework

- ○ Strongly Agree
- ○ Agree
- ○ Undecided
- ○ Disagree
- ○ Strongly Disagree

UNIVERSITEIT GENT

Please explain your answer and provide any additional suggestions you may have.

_____

_____

_____

_____

_____

PTP (5) Increased scope leading to further processing incompatible with the initial purpose

Problem: New types of privacy threats could result from the ability of big data to re-contextualise data combined with the increasing exposure of personal data in data-fertile fields such as healthcare, manufacturing, banking and the public sector.

Solution: The impact of the increased scope and the possible consequences of incompatible processing should be assessed in accordance with the WP29 Opinion on Purpose Limitation [1] and become an integral part of the DPIA Guidelines paper. Ideally, the points raised in Annex 2 of [1] will be addressed through a complementary assessment that examines the compatibility of the data processing operations with the information found in the consent model proposed in PTP (1).

[1] WP29. (2013). Opinion 03/2013 on purpose limitation

UNIVERSITEIT GENT

- ○ Strongly Agree
- ○ Agree
- ○ Undecided
- ○ Disagree
- ○ Strongly Disagree

Please explain your answer and provide any additional suggestions you may have.

_____

_____

_____

_____

_____

PTP (9) Treatment of indirect privacy harms

Problem: Several authors argue that societal and ethical concerns should also be addressed when dealing with big data. For example, the exploitation of big data in healthcare – especially during the COVID-19 outbreak has generated significant ethical challenges that, apart from unlawful practices, can affect societal norms and values.

Solution: Societal and ethical impact concerns of Big Data Analytics could be addressed by assessing the degree of fairness, accountability and transparency in the processing operations. As they may arise at different stages of a Big Data Analytics project, the DPIA Guidelines could encourage the use of a framework such as the Fair, Accountable and Transparent 'FAT Flow' [1], which in addition could also greatly help data controllers to identify and mitigate potential

privacy harms.

[1] Martens, D. (2020). FAT Flow: A Data Science Ethics Framework

- ○ Strongly Agree
- ○ Agree
- ○ Undecided
- ○ Disagree
- ○ Strongly Disagree

Please explain your answer and provide any additional suggestions you may have.

_____

_____

_____

_____

_____

End of Block: DPIA Improvements

UNIVERSITEIT GENT

Start of Block: Miscellaneous

Purpose of our Delphi Study

Before ending this survey, we would like to remind you of the purpose of the Delphi study, which was to validate and possibly expand the PTPs we have identified in our paper [1] and by doing so suggest improvements to the DPIA guidelines that would make them more relevant to applications involving Big Data Analytics.

We would therefore like to ask you to add some general comments on aspects of importance for our research on this topic.

[1] G. Georgiadis and G. Poels, “Towards a Privacy Impact Assessment Methodology to Support the Requirements of the General Data Protection Regulation in a Big Data Analytics Context : A Systematic Literature Review,” Publ., Computer Law & Security Review 2022

(optional) Please add any general comments below.

_____

_____

_____

_____

_____

End of Block: Miscellaneous