Legitimate Interests and Integrated Risk and Benefits Assessment

A Framework for Determining if Processing as Permitted by Legitimate Interests is Legal, Fair and Just

Dated: 10 September 2017

Table of Contents

The Information Accountability Foundations wishes to thank the many stakeholders that have been involved in this project beginning with the initial work on ethical assessments. Those stakeholders have included enforcement agencies, civil society, academia and business. Work conducted in Canada with a grant from the Office of the Privacy Commissioner helped fund earlier work that was most helpful in the current project. Martin Abrams, Peter Cullen, and Lynn Goldstein are the principle IAF project strategists, and responsible for this content.

I. EU LEGITIMATE INTEREST AND DPIA PROJECT OVERVIEW & SUMMARY

The EU General Data Protection Regulation (GDPR) requires organisations that collect and use data in a robust and an innovative manner to conduct numerous assessments. The GDPR contains many review and documentation requirements. At the most basic level, organisations will need to understand the risks associated with a processing, and whether a full data protection impact assessment (DPIA) is required. Second, if the legal basis for processing the data would be legitimate interests, then a balancing process would be required that examines the full range of rights and interests of all stakeholders to ensure interests are not overridden by the interests or fundamental rights and freedoms of the data subject. This balancing process is an assessment.

The Information Accountability Foundation (IAF) project charge has been to develop a trustworthy legitimate interest assessment process, one that isolates the issues that need to be considered so that processing is in balance. IAF's work has demonstrated that many of the same issues that come into play to determine if a processing is risky to individuals are the same issues that need to be considered when determining that legitimate interest is a lawful basis for a processing. While the IAF charge has been to develop trustworthy legitimate interest assessments, the IAF's business process experience has led it to conclude that legitimate interest is most efficiently assessed as part of an integrated comprehensive data impact assessment (EU ICDIA). For regulatory reporting processes, outputs could be specific to legitimate interests. However, the process itself would also operate as the questions necessary to understand risks, benefits and mitigations relevant to DPIAs. In the end, an organisation engaging in high-risk processing will need to evaluate the origin, nature and severity of the risk to data subjects, and those fact patterns will be used to satisfy numerous GDPR requirements.

The GDPR respects all interests and fundamental rights. These rights and interests go beyond autonomy and include, for example, safety, better education and healthcare, shared benefits from technology and more robust opportunities. This breadth of coverage means consideration of what is legitimate or not cannot be a simple fulcrum looking to balance interests between a controller and a single data subject's desire for autonomy but rather must be a variable analysis.

Likewise, understanding whether processing will create substantial risks for data subjects requires a consideration of the nature of risk. One's sense of what is a risk is based on shared societal values. Data protection risks traditionally have been seen as harms-based, but the concept of free flow of data is predicated on the risks associated with lost opportunity as well.

If one is looking at the full range of interests and measuring risk fully, then a set of values to evaluate against is needed. Five core values, (i) Beneficial, (ii) Progressive, Necessary and Proportional, (iii) Sustainable, (iv) Respectful of Obligations, (v) Fairness – Reasonable Expectations of the Data Subject,[1] can be used to serve this evaluative purpose. Additionally, it is necessary to define the desired outcome of these assessments and that they are seen as responsible; the concept of legal, fair and just is a useful approximation of these outcomes.

[1] See GDPR Risk Assessments – DPIAs and Legitimate Interests – to Isolate Risk and Benefits and Demonstrate Compliance for a discussion of these values.

This project of the IAF, conducted with input from business leaders and data protection authorities,[2] develops a framework, the EU ICDIA, for trusted accountability when organisations use legitimate interest as the legal basis for processing data in innovative and intensive ways, particularly when using advanced, big data analytics, and/or when conducting DPIAs for high-risk processing. The EU ICDIA helps an organisation determine whether its processing is legal, fair and just and demonstrate how this determination was reached. If done correctly, the EU ICDIA also enables transparency within the organization, and the outcome enables transparency to data subjects, to society, and to regulators.

This project and document contains three (3) parts:

1. **The GDPR Integrated Risk Assessments - DPIAs and Legitimate Interests – To Isolate Risks and Benefits and Demonstrate Compliance,** a theory document that explains the legal concepts that link to and support the EU ICDIA.
2. **The EU ICDIA Summary Chart** that demonstrates the integration of legitimate interest assessments and DPIAs and key evaluation points.
3. **The EU ICDIA model assessment** that helps make clear the questions necessary to raise the key issues. The EU ICDIA [3] assessment is as it states: a model. It is IAF's belief that organisations will use this model to develop their own assessment or evaluate assessments or tools developed by others. This model assessment integrates the legitimate interest assessment and the DPIA. IAF believes that most organisations, when using data in a new way, will need a triage process to determine what assessments should be conducted (see EU ICDIA Process Flow above). In some cases, the new data uses are similar to ongoing processes and can effectively be governed by consent. In others, a full legitimate interest assessment and/or DPIA is necessary. IAF believes an integrated process will be followed by most organisations.

[2] The IAF is solely responsible for its content.

[3] EU ICDIA is based on a technology assisted tool developed by TrustArc. Other market participants such as Nymity are developing technology assisted assessment tools that encompass the key balancing concepts

II. GDPR INTEGRATED RISK ASSESSMENTS - DPIAs AND LEGITIMATE INTERESTS – TO ISOLATE RISKS AND BENEFITS AND DEMONSTATE COMPLIANCE

Forward

The Information Accountability Foundation (IAF) was charged with creating a General Data Protection Regulation (GDPR) focused legitimate interest assessment process based on the IAF's Unified Ethical Frame for Big Data Analysis. As IAF worked with stakeholders, it became clear that the fact pattern that needed to be developed for the legitimated interest assessment was also the fact pattern necessary to determine whether a data protection impact assessment (DPIA) was necessary and what the key risk and benefit issues would be for both assessments. Therefore, IAF's scope has changed from just a legitimate interest assessment to rather legitimate interest as part of an integrated comprehensive assessment that includes a DPIA as well. The output from such an analysis would then be mapped to the various demonstration requirements contained in the GDPR. The IAF is calling the new process an EU Integrated Comprehensive Data Impact Assessment (EU ICDIA).

Introduction

The European Commission's Digital Single Market Strategy has three priority areas: better access for consumers and businesses to digital goods and services across Europe, shaping the right environment for digital networks and services to flourish, and creating a European Digital Economy and society with growth potential.[4] The European Union General Data Protection Regulation (GDPR) is intended to contribute to the accomplishment of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market.[5] The GDPR will strengthen consumer trust in the digital economy and make it easier for European Union (EU) and foreign companies to carry out their business activities in the EU.[6]

Protection of natural persons in relation to the processing of personal data is a fundamental right.[7] The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.[8] Likewise, the right to privacy – respect for everyone's private and family life, home and correspondence – is considered a relative or qualified human right.[9] The GDPR respects all fundamental rights and observes, in particular, the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and

[4] European Digital Single Market Factsheet
[5] GDPR Recital 2
[6] European Commission – Fact Sheet – Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers
[7] GDPR Recital 1
[8] Id. Recital 4
[9] Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217) at 11

information, freedom to conduct a business, the right to effective remedy and to a fair trial, and cultural, religious and linguistic diversity.[10]

For the Digital Single Market Strategy to work, personal data must be able to be used in a manner that meets the needs of both individuals and commerce. The flexibility built into the GDPR is intended to do just that. Importantly, several Articles of the GDPR call for assessments.[11] Since the requirements of each of these assessments overlap, in practice organisations will want to implement these assessments in an integrated manner. The requirements for these assessments are similar, and therefore these assessments can be conducted either separately or when appropriate incorporated together. When conducted in an integrated manner, the assessment process is more efficient and requirements are not unnecessarily repeated, thus meeting two of the goals of the Digital Single Market Strategy - strengthening consumer trust and making it easier for companies to carry out their business activities. Assessment outputs could be structured to meet the specific demonstration needs associated with the various GDPR Articles.

GDPR Basic Processing Requirements

The basic processing requirements for GDPR assessments are the same.

Personal data[12] must be processed lawfully, fairly and transparently (lawfulness, fairness and transparency principle), and the processing of personal data is subject further to the principles of purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality.[13] The controller is responsible for and must be able to demonstrate compliance with these principles (accountability principle) (collectively data processing principles).[14]

The accountability principle focuses on two main elements: (1) The need for a controller to take appropriate and effective measures to implement data protection principles.[15] The GDPR requires data controllers to implement certain measures (e.g. implementation of data protection by design and by default,[16] conduct of data protection impact assessments,[17] designation of the data protection officer[18]), and (2) The need to demonstrate upon request that appropriate and effective measures have been taken.[19] Thus, the controller must provide evidence that that these appropriate and effective measures have been taken.[20]

Processing is lawful only if at least one of the following applies: legitimate interest (processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party,

[10] GDPR Recital 4
[11] Id. Articles 6(1)(f), 35(7), 49(1) and 88(2). See WP 217 at 11-12
[12] Processing of sensitive data is prohibited. GDPR Article 9(1)
[13] Id. Article 5(1)
[14] Id. Article 5
[15] Article 29 Data Protection Working Party Opinion 3/2010 on the principle of accountability (WP 173) at 9
[16] GDPR Article 25
[17] Id. Article 35
[18] Id. Article 37
[19] WP 173 at 9
[20] Id.

except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child)[21], consent[22], contract, legal obligation, vital interest or public task.[23] Processing on the basis of legitimate interest requires a balancing of the legitimate interests of the controller, or any third parties to whom the data are disclosed, against the interests or fundamental rights of the data subject.[24]

Processing must be compatible for any purpose for which the personal data have been collected. Where the processing is for a purpose other than that for which the personal data have been collected, and is not based on the data subject's consent, the controller, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data were initially collected, must "take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed . . .;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation."[25]

This list of key factors, to be used in order to assess compatibility, is not exhaustive and attempts to highlight the most typical factors that may be considered in a balanced approach: neither too general so

[21] GDPR Article 6(1)(f). Centre for Information Policy Leadership Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR (CIPL Recommendations) at 15-16 (Legitimate interest is an essential processing ground in the modern ages. It ensures that the GDPR remains future-proof and technology neutral. It enables ongoing delivery and improvement of products and services, and new and innovative uses of data, while ensuring organizational accountability and respecting data protection rights of individuals.)

[22] GDPR Article 6(1)(a); CIPL Recommendations at 2 (Using consent as a legal basis for processing is challenging given the complexity of today's data flows and uses. The digital ecosystem raises the importance of other grounds for processing such as legitimate interest. Legitimate interest may be the most accountable ground for processing in many contexts, as it requires an assessment and balancing of the risks and benefits of processing for organisations, individuals and society.)

[23] GDPR Article 6(1)(b)-(e). Transparency is required regarding the legal basis for the processing. Id. Articles 13-14. How to achieve effective transparency is work that needs to be done but is beyond the scope of this paper.

[24] *See* Id. Recital 47. *See also* WP 217 at 3; *Valsts policijas Rīgas regiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme',* CJEU 4/5/17 Case C13/16) (Three cumulative conditions must be met for the processing of personal data under the legitimate interest basis to be lawful: (1) pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; (2) the need to process personal data for the purposes of the legitimate interests pursued; and (3) that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence. The third condition is where the 'balancing of the opposing rights and interests at issue' are addressed. Setting this balance depends "on the specific circumstances of the particular case."); Data Guidance, Italy: Garante's decision "provides useful element to companies looking to rely on legitimate interests" 1/6/17 (Under the GDPR, any organisation, before starting any data processing based on legitimate interests, must not only assess if it has properly considered all the risks at stake, but also collect adequate elements to be in a position to prove the relevant interests have been well balanced.)

[25] GDPR Article 6(4); Recital 50

as to be meaningless nor too specific so as to be overly rigid.[26] These key factors focus a compatibility determination.[27]

Relationship Between Two Assessments: Legitimate Interest Assessments and DPIAs

The requirements of legitimate interest assessments and DPIAs are similar.

Legitimate Interest Assessments

Article 6(1)(f) allows processing subject to a balancing test which weighs the legitimate interests of the controller – or the third party or parties to whom the data are disclosed – against the interests or fundamental rights of the data subjects.[28] The existence of a legitimate interest needs careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.[29] The interests and fundamental rights of the data subject could override the interest of the data controller where personal data are processed in circumstances where data subjects do not expect further processing.[30] The processing of personal data for the purposes of preventing fraud and for direct marketing purposes are regarded as carried out for a legitimate interest.[31] Providing detailed and exhaustive lists of situations in which the legitimate interests of the controller as a rule prevail over the fundamental rights of the data subject or vice versa could risk being misleading, unnecessarily prescriptive, or both.[32] On the other hand, if the assessment were to be made case by case without any further guidance inconsistent application and lack of predictability could result.[33] Rather, further guidance regarding how to conduct an assessment balancing these interests and rights is necessary.[34]

[26] Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation (WP 201) at 3
[27] Id. at 23; Baker McKenzie Hot Topics 5/17) (The German Parliament approved the draft of a new Federal Data Protection Act (New Act) on April 27, 2017 in order to align the German data protection law with the requirements of the GDPR and to make use of the opening clauses of the GDPR. The German Federal Council approved the New Act on May 12, 2017, and the New Act will come into effect on May 25, 2018, the same date as the GDPR. Section 24 of the New Act provides that personal data may be processed for a purpose different than the purpose for which it was collected if this is necessary to (1) defend against risks related to governmental or public safety or for criminal prosecution, or (2) exercise, establish, or defend against civil claims, unless the interests of the data subject prevail. Thus, unlike GDPR Article 6(4), in Germany, the legitimate interest test will be used to justify further processing in the two specified circumstances.)
[28] WP 217 at 4
[29] GDPR Recital 47
[30] Id.
[31] Id.
[32] WP 217 at 12. *See, e.g.* id. at 57-68; Article 29 Data Protection Working Party Opinion 2/2017 on data processing at work (WP 249) at 10-22.
[33] WP 217 at 12.
[34] Id. See the EU ICDIA accompanying this paper (pages 22-54).

The balancing test called for under Article 6(1)(f) is not a straightforward one which would simply consist of weighing two easily quantifiable and easily comparable 'weights' against each other.[35] Rather, carrying out the balancing test requires an assessment taking into account a number of factors.[36] The balancing of the opposing rights and interests concerned depends, in principle, on the individual circumstances of the particular case in question and in the context of which the person or the institution which carries out the balancing must take account of the significance of the data subject's fundamental interests and rights.[37] While the outcome of the balancing test largely determines whether Article 6(1)(f) may be relied upon as a legal ground for processing, it also should be seen as a tool for accountability and should help organisations build compliance at the outset and demonstrate compliance at a later date.[38]

Data Protection Impact Assessments

DPIAs are based on many of the same factual drivers as legitimate interest assessments. DPIAs should be carried out when the controller is engaging in high risk processing in order to evaluate, in particular, the origin, nature, particularity and severity of that risk.[39] Article 35(3) of the GDPR contains a list of circumstances when DPIAs are required, and the Guidelines contain examples of each of these circumstances.[40] However, the WP 29 emphasizes that this list of circumstances is non-exhaustive, and additional factors are mentioned by the WP 29.[41] Indeed, the WP 29 recommends that DPIAs should be seen as a tool for accountability and could be used in wider situations as well.[42] In the view of the WP 29, conducting DPIAs will help organisations build compliance at the outset and demonstrate compliance at a later date.[43]

Article 35(7) of the GDPR sets out the minimum content of DPIAs:

"(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

[35] WP 217 at 23
[36] Id.
[37] *See* European Data Protection Supervisor Opinion 7/2015 Meeting the challenges of big data (7/15 EDPS Opinion) at 12 (Data processing whose benefits are general/societal must be distinguished from those that merely provide economic benefits to those processing the data. The potential impact on the individuals concerned must be assessed and those two must be carefully balanced as well as other relevant factors.) (citing WP 217); *Associación Nacional de Establecimientos Financieros de Crédito & Federación de Comercio Electrónico y Marketing Directo v. Administración del Estado*, CJEU, 24/11/11; CIPL Recommendations at 17-18
[38] *See* Article 29 Data Protection Working Party 29 (WP 29) Guidelines on DPIA and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (Guidelines) at 4; CIPL Recommendations at 16
[39] Guidelines at 4.; GDPR Recital 84
[40] GDPR Article 35(3); Guidelines at 10.
[41] Guidelines at 9
[42] Id. at 4
[43] Id.; Bird & Bird, Article 29 Working Party issues draft guidelines on Data Protection Impact Assessments and high risk processing 13/4/17

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purpose;

(c) an assessment of the risks to the rights and freedoms of the data subjects . . .;

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the [GDPR] taking into account the rights and legitimate interests of data subjects and other persons concerned."[44]

Thus, under Articles 6(1)(f) and 35(7),[45] there is a four-step analysis: (1) the activity involves legitimate interest and/or high risk processing, (2) risks and benefits are assessed, (3) if risks outweigh benefits, risks are further assessed to determine whether they can be further reduced, and (4) compliance with all other provisions of the GDPR.[46]

Incorporation of Five Key Values into the EU ICDIA

As discussed above, guidance regarding how to conduct assessments under the GDPR is necessary. Organisations in all sectors have been engaging in the processing of personal data for decades in order to manage their employment relationships, conduct research and development, prevent fraud, secure systems, and operate and provide products and services. In addition to legitimate interest assessments and DPIAs, robust processing requires an assessment. In order to establish that their particular types of processing are in compliance with the data processing principles and the necessity and proportionality obligations and based on lawful grounds, organisations may conduct an assessment that considers the various interests, rights and freedoms, always considering the overarching ethical goals of legal, fair[47] and just[48]. The IAF with the assistance of former data protection authorities, data scientists and business representatives has developed such an assessment that began with a paper on conflicting ethical frames.[49] This paper resulted in the harmonization of ethical frames into five key values: (i)

[44] GDPR Article 35(7)

[45] The assessment in Articles 6(1) and 35(7) is also similar to the assessment that is required in Article 49(1) of the GDPR in the case of transfers based on a compelling legitimate interest and in Article 88(2) of the GDPR in relation to the protection of legitimate interests in respect to the processing of personal data in the context of employment.

[46] See EU ICDIA process flow on page 24 that further breaks down this analysis. William Fry, EU's Top Court Clarifies 'Legitimate Interest Test' for Data Processing 15/5/17 (If the data subject objects, then under GDPR Article 21(1) the controller can no longer process the personal data unless the controller demonstrates "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.") The assessment set forth in Article 21(1) is part of the legitimate interest assessment and the DPIA.

[47] GDPR Recital 39

[48] Id. Recital 2; WP 203 at 7 (The term "just" incorporates Article 8 of the European Convention on Human Rights which infers justification for any interference with privacy.)

[49] IAF began the Big Data Initiative in early 2014. IAF brought together numerous thought leaders, including former data protection commissioners, to discuss the issues related to trustworthy big data analytics. Based on that dialogue, IAF published "A Unified Ethical Frame for Big Data Analysis" (Unified Ethical Frame) in October 2014. IAF also organized a plenary session at the 36th International Conference of Data Protection and Privacy Commissioners on the ethical use of big data. In 2015, IAF continued the Big Data Ethics Initiative with the creation of a model assessment framework for digital marketing. That same

Beneficial, (ii) Progressive, (iii) Sustainable, (iv) Respectful, and (v) Fair. The use of these values assists organisations in determining whether complex processing is fair and just to the stakeholders impacted. These five values, therefore, are reflected in IAF's Comprehensive Data Impact Assessment (CDIA), that was developed as part of its Effective Data Protection Governance Project.[50] The CDIA supplements and helps practical implementation of Articles 6(1)(f) and 35(7) of the GDPR,[51] resulting in the development of the EU ICDIA. Consideration of these five values enhances an organisation's compliance program in meeting the GDPR goal of fair processing and its observance of the accountability principle.[52] Ultimately, by providing an assessment for establishing that processing is in compliance with the data processing principles and based on lawful grounds, the EU ICDIA helps an organisation, as part of its compliance program, determine whether its processing is legal, fair and just and demonstrate how that determination was reached. When determining whether processing achieves the ethical goals of legal, fair and just[53], the individual's rights are paramount to the interests of the organisation.[54]

To understand these five values, it is important to appreciate that processing may not be equally impactful on the individuals to whom the data pertains. The WP 29 encourages the development of sector-specific DPIA frameworks.[55] By way of example, the EU ICDIA may be used as a DPIA for high-risk processing, including big data analytics and other data intensive processing.[56] Continuing with this example, each of the five values are defined in the context of legitimate interest processing in the EU and then illustrated in the context of an EU ICDIA of big data analytics. However, the five values are not limited to big data analytics; indeed, they are applicable to any of the circumstances when DPIAs are required under the Guidelines.[57]

Big data analytics refer to the gigantic digital data assets held by corporations, governments and other large organisations which are then extensively analysed using computer algorithms.[58] Big data relies on the increasing ability of technology to support the collection and storage of large amounts of data but also to analyse, understand and take advantage of the full value of data (in particular using analytics applications).[59] The expectation from big data is that it may ultimately lead to better and more informed decisions.[60] Big data analytics usually can be separated into two phases: "thinking with data" and "acting with data".[61] Generally, "thinking with data", like research, is where new insights, which go

---

year, IAF authored a paper on how such an assessment process might be enforced by regulatory authorities with different mandates. A session to explain the oversight of big data was organized by IAF as a side event at the 37th International Conference of Data Protection and Privacy Commissioners. The participation by the Office of the Privacy Commissioner of Canada in the Big Data Ethics Initiative led to the Canadian Big Data Assessment that is the predecessor to the Legitimate Interest Assessment. Concepts explored in the Unified Ethical Frame are reflected in the ethics opinions issued by the European Data Protection Supervisor. (Opinion 4/2015 Towards a new digital ethics and 7/15 EDPS Opinion)

[50] IAF website

[51] See note 45 *supra.*

[52] GDPR Article 5(2)

[53] 7/15 EDPS Opinion at 16

[54] *See* GDPR Recital 47: Id. Article 35(7)

[55] Guidelines III. C. at 16

[56] Id. III. B. at 8-9 (Big data is data processing on a large scale and therefore is subject to a DPIA.)

[57] Id. at 10

[58] Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation (WP 203) Annex 2 at 45

[59] Id.

[60] Id.

[61] These concepts are a refinement of the two-phase process, knowledge discovery and application, discussed in "Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance - A Discussion Document. February 2013" Centre for Information Policy Leadership

beyond experience and intuition and come instead from correlations among data sets, are discovered. "Acting with data," generally, is where these insights are put into effect and where individuals may be affected as these insights are employed in an individually unique manner.

The obligations of legal, fair and just apply to both the "thinking" and "acting" with data phases. While the "acting with data" phase often is individually impactful,[62] the "thinking with data" phase may not be as individually impactful if aggregate data is used.[63] The two phases may be governed differently by data protection law (e.g. traditional methodologies such as consent may be more effective when "acting with data"). Understanding the risks and benefits in both phases is critical (the risks related to false insights usually are the primary concern in the "thinking with data" phase). It is necessary to distinguish between "thinking with data" and "acting with data" when considering the five key values in connection with big data analytics.[64]

(i) Beneficial

All processing of data related to individuals creates risks for some stakeholders and benefits for the same or other stakeholders. The term "stakeholder" can be very broad and includes both individuals and society. The beneficial value requires an organization to understand those risks and benefits.

Purpose specification is an essential condition to processing personal data and determines the relevant data to be collected, retained and processed for the chosen purpose.[65] The purpose must be sufficiently defined to enable implementation of any necessary data protection safeguards and to delimit the scope of the processing operation; it must be clearly revealed, explained or expressed in some intelligible form; it must be in accordance with all provisions of applicable data protection law as well as other applicable laws.[66]

The concept of 'interest" is closely related to, but distinct from, the concept of 'purpose.'[67] 'Purpose' is the specific reason why the data are processed; the aim or intention of the data processing.[68] An interest is the broader stake that a controller may have in the processing or the benefit that the controller derives - or the society might derive – from the processing.[69] If the controller – or the third party in the case of disclosure – can pursue any interests, provided they are not illegitimate, then all categories of interests of the data subject should be considered as well (the adjective 'legitimate' does not precede the 'interests' of the data subjects and therefore individual interests and rights has a wider

[62] Where organisations "act with data," individuals have the ability to opt in.
[63] *See* GDPR Recitals 32, 50 (Consent covers all processing carried out for the same purpose or purposes. If an organisation's "thinking with data" is compatible with the purposes for which the personal data were originally collected, then the organisation can assume the individual has consented.)
[64] The GDPR applies in both phases. GDPR Article 89; Id. Recital 159
[65] WP 203 at 12, 21 (The purposes of processing must be specified prior to, and in any event, not later than, the time when collection of personal data occurs. Any processing following collection, whether for the purposes initially specified or for any additional purposes, must be considered further processing and must thus meet the requirement of compatibility.)
[66] Id. at 12, 17, 20
[67] WP 217 at 24; Information Commissioner's Office, Big data, artificial intelligence, machine learning and data protection (ICO) at ¶¶ 76-82
[68] WP 217 at 24
[69] Id.

scope).[70] Broadly stated, the purpose of the EU ICDIA is achieving the benefits that come with reducing the possible risks.[71] Minor and not very compelling legitimate interests of the controller may, in general, only override the interests and rights of data subjects where the impact on these rights and interests are even more trivial.[72] Important and compelling legitimate interests of the controller subject to safeguards and measures may, on the other hand, in some cases justify even significant intrusion into privacy or other significant impact on the interests or rights of the data subject.[73] Safeguards can reduce the undue impact on data subjects and thereby change the balance of rights and interests to the extent that the data controller's interests will not be overridden.[74] Requiring data subjects' interests as well as 'fundamental rights and freedoms' to be taken into account provides more protection for the data subject.[75] A key factor to consider when applying the balancing test is whether the data subject or society as a whole will benefit from the processing.[76] A similar analysis applies when conducting a DPIA because a DPIA requires assessing necessity and proportionality of the processing operations in relation to the purpose, assessing risks to the rights and freedoms of data subjects, and assessing measures envisaged to address risks.[77] Thus, legitimate interest assessments and DPIAs require an assessment and balancing of the risks and benefits of the processing for the organisation, individuals and society.[78]

Big data analytics and other data intensive processing, if done responsibly, can deliver significant benefits and efficiencies for society and individuals.[79] When "thinking with data" and "acting with data", an organisation is required to define the benefits that will be created by the analytics and to identify the parties that gain tangible value from the effort. The act of big data analytics may create risks for some individuals. Those risks must be counter-balanced by the benefits created for or the interests of all individuals and/or society as a whole.[80] Benefits to the organisation cannot equal or outweigh those of the individual.[81] Indeed, the organisation will need to consider whether it will be necessary to set aside its own interests after "thinking with data" with aggregate data.[82]

To define benefits, one must have an understanding of why the data is being processed.[83] While big data analytics do not always begin with a hypothesis, they usually begin with a sense of intent about the type of problem to be solved.[84] Data scientists, along with others in an organisation, should be able to define the usefulness or merit that comes from solving the problem, so it might be evaluated appropriately.

---

[70] Id. at 30
[71] See GDPR Article 35(7)
[72] WP 217 at 30
[73] Id.
[74] Id. at 31
[75] Id. at 29
[76] Id. at 47 n. 109; CNIL Methodology for Privacy Risk Management (Translation of June 2012 edition) 2.1 at 11
[77] GDPR Article 35(7)
[78] CIPL Recommendations at 3 (Legitimate interest also requires the implementation of appropriate mitigations to reduce or eliminate any unreasonable risks. This places the burden of protecting individuals on the organization and shifts it away from individuals. Organisations are in the best position to undertake a risk/benefits analysis and to devise appropriate mitigations, and individuals should not be overburdened with making these assessments and informed choices for all digital interactions and processing of their personal information.)
[79] 7/15 EDPS Opinion at 4
[80] WP 217 at 23
[81] Id. at 26
[82] Id.
[83] Id. at 24
[84] Id.

The risks[85] also should be clearly defined so that they may be evaluated as well.[86] If the benefits that will be created are limited, uncertain, or if the parties that benefit are not the ones at risk from the processing, those circumstances should be taken into consideration, and appropriate safeguards for the risk should be developed before the analysis begins.[87]

(ii) Progressive, Necessary and Proportional

The processing of data that pertains to individuals should only be conducted if it improves on existing procedures. The progressive value means that processing should be necessary and proportional.[88] Necessary means the processing of personal data must be essential for the purpose pursued by the controller.[89] Proportional means the controller should consider whether other less invasive means are available to serve the same end.[90]

For the controller's legitimate interest to prevail, the data processing must be 'necessary' and 'proportionate' in order to exercise the fundamental right concerned.[91] This condition requires a connection between the processing and the interests pursued.[92] It is the controller who has the responsibility to evaluate whether the processing is necessary and proportionate.[93] Likewise a DPIA must assess the necessity and proportionality of the processing operations in relation to the purposes of the processing, and it is the controller who remains ultimately accountable to make sure that the DPIA is carried out.[94]

Since bringing large and diverse data sets together and looking for hidden insights or correlations may create some risks for some individuals, the value from big data analytics should be materially better than not using big data analytics. If the anticipated improvements can be achieved in a less data-intensive manner, then less intensive processing should be considered.[95] Precision is not required. One might not know the level of improvement in the "thinking with data" phase. Yet, by the time one is proposing to move to the "acting with data" phase, the organisation should be better equipped to measure the level of improvement. This application of new learnings to create materially better results is what drives innovation.

[85] An articulation of big data risks is set forth in the EU ICDIA in Part B
[86] GDPR Recital 83; Guidelines III. C. at 15
[87] WP 217 at 31 and n.67; Guidelines III. C. at 15
[88] Article 29 Working Party Document 01/2016 on the justification of interference with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (WP 237) at 7. *Also see* the "proportionality test" required by the Spanish Constitutional Court before implementing any monitoring: Is the measure suitable (i.e., adequate to achieve the aims pursued); is the measure necessary (i.e., is there another measure less intrusive to the employees' privacy that would achieve the same aims); is the measure justified and balanced?
[89] WP 217 at 29
[90] Id.
[91] Id. at 34
[92] Id. at 29
[93] Id. at 43
[94] GDPR Article 35(7)(b); Guidelines III, C. at 13
[95] WP 217 at 43

Progressive must be assessed in the context in which the processing takes place.[96] There are examples of big data being used to reduce congestion, manage disaster relief and improve medical outcomes where the level of improvement would not have been possible without big data analytics. However, there are other examples where organisations may analyze data and achieve only marginal improvements but only use big data analytics because big data is new and interesting. If there are other methods that will accomplish the same objectives, organisations should consider pursuing those other methods rather than using big data analytics to produce the same or lesser results with greater risks.[97]

(iii) Sustainable

The sustainable value requires an organization to understand whether data used for "thinking with data" will still be available legally for "acting with data". Furthermore, sustainable requires an organization to understand the time-period for which data, and the processes based on that data, might be accurate.

Sustainable is grounded in the accuracy and lawfulness, fairness and transparency principles relating to the processing of personal data.[98] Personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject and be accurate and where necessary kept up to date.[99]

The nature of the data, the status of the data controller and the status of the data subject, the nature of the relationship or the service provided, and the applicable legal or contractual obligations (or other promises made at the time of collection) could affect the impact of the processing on the interests or fundamental rights of the data subject.[100] Additional safeguards applied by the controller (e.g., pseudonymisation and encryption) may ensure better protection of personal data.[101] Similarly, DPIAs should take into account the nature, scope, context, and purposes of the processing and should include the measures, safeguards and mechanisms envisaged for risks.[102]

With respect to data analytics, sustainable covers two issues. The first is understanding how long an insight might be effective, while the second relates to whether the data used for the insight might be available when acting with data. Algorithms for data analytics have an effective half-life – a period in which they effectively predict future behavior. Some are very long; others are relatively short. Big data analysts should understand this concept and articulate their best understanding of how long an insight might endure once it is reflected in application. Big data insights, when placed into production, should provide value that is sustainable over a reasonable time frame. Considerations that affect the longevity of big data analytics include whether the source data will be available for a period of time in the future,

[96] GDPR Recital 47
[97] WP 217 at 29.
[98] GDPR Article 5(1) (a), (d); ICO at ¶¶ 50–53, 91-96
[99] GDPR Article 5(1); Id. Recital 39
[100] WP 217 at 38, 40
[101] Id. at 42
[102] GDPR Recital 90

whether the data can be kept current, and whether the discovery may need to be changed or refined to keep up with evolving trends and individual expectations.

There are situations where data, particularly anonymised or aggregated data, might be available for the "thinking with data" phase but would not be available in the "acting with data" phase because of legal or contractual restrictions. These restrictions affect sustainability.[103]

(iv) Respectful of Obligations

Respectful relates directly to the context in which the data originated and whether that context is reasonable and to the contractual or notice related restrictions on how the data might be applied. It also relates to any processing following collection since further processing must be compatible.[104] The fact that further processing is for a different purpose does not necessarily mean that it is automatically incompatible; further processing needs to be assessed on a case-by-case basis.[105]

The existence of a legitimate interest needs a careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.[106] Taking into account the nature, scope, context and purposes of the processing is an important part of a DPIA as well.[107] Establishing the context means taking into account the nature, scope, context and purposes of the processing and the sources of the risk.[108]

Big data analytics may affect many parties in many different ways.[109] Those parties include individuals to whom the data relates, organisations from whom the data originates, organisations that aggregate the data and those that might regulate the data.[110] All of these parties have interests in the data that must be taken into consideration and respected.[111] The EU ICDIA can help organisations understand what is respectful.[112] When determining whether big data activities are respectful, the individual's rights may be paramount to the interests of the organisation.[113]

Organisations using big data analytics should understand and respect the interests of all the parties involved in, or affected by, the analytics, and that in certain circumstances the rights of the individual have priority.[114] Anything less would be disrespectful.

---

[103] WP 217 at 42
[104] GDPR Article 6(4); WP 203 at 21
[105] Id.
[106] Id.; GDPR Recital 47
[107] GDPR Recital 90
[108] GDPR Articles 6(4) & 35(1); Guidelines III. C. at 15
[109] What is respectful may depend also on whether the activity is in the "thinking" or "acting" with data phase. In the "thinking with data" phase, further processing might be compatible while in the "acting with data" phase, the same further processing might not be considered compatible.
[110] WP 203 at 45-47
[111] Id.
[112] *See* WP 217 at 40
[113] Id. at 33
[114] Id.

(v) Fairness – Reasonable Expectations of the Data Subject

While "respectful" speaks to the conditions related to, and the processing of, the data, "fair" and "just" relate to the impacts of that processing.[115] In assessing the impact of the processing, both positive and negative consequences should be taken into account.[116] 'Impact' is a much broader concept than harm or damage to one or more specific data subjects.[117] Impact covers any possible (potential or actual) consequences of the data processing and encompasses the various ways in which an individual may be affected – positively or negatively – by the processing of his or her personal data.[118] The purpose of the balancing exercise is not to prevent any negative impact on the data subject; rather, its purpose is to prevent disproportionate impact.[119] The more significant the impact on the data subject, the more attention should be given to relevant safeguards.[120]

Fair, when balancing interest, is concerned with the consequences of the data processing activity for data subjects.[121] These consequences may include potential future decisions by third parties and situations where the processing may lead to the exclusion of, or discrimination against, individuals, defamation, or more broadly, situations where there is a risk of damaging the reputation, negotiating power, or autonomy of the data subject.[122] In addition to adverse outcomes that can be specifically foreseen, broader emotional impacts need to be taken into account.[123] The chilling effect on protected behavior must also be given due consideration.[124] Correspondingly, the DPIA is a tool for managing risks to the rights and freedoms of data subjects, and thus takes their perspective.[125]

"Fair" with respect to big data analytics relates to the insights and applications that are a product of big data. EU law prohibits discriminatory practices based on race, national or ethnic origin, colour, religion, age, and sex.[126] Yet, big data analytics may predict those characteristics without actually looking for fields labeled race, national or ethnic origin, colour, religion, age, or sex. The same can be said about genotypes, particularly those related to physical characteristics. Inferring characteristics and using them to make decisions based on prohibited grounds is not just. Big data analytics, while meeting the needs of

[115] GDPR Recital 39; ICO at ¶¶ 31-37
[116] WP 217 at 37
[117] Id.
[118] Id.
[119] Id. at 41
[120] Id. at 42
[121] Id. at 33
[122] Id. at 37
[123] Id.
[124] Id.
[125] Guidelines III, C at 15
[126] *E.g.* Racial Equality Directive, 2000/43/EC; Employment Equality Directive, 2000/78/EC; Gender Equality Directive, 2006/54/EC (in relation to employment); Gender Equality Directive, 2004/113/EC (un relation to goods and services); Gender Equality Directive, 79/7/EC (in relation to social security)

the organisation that is conducting or sponsoring the processing, must be fair to both the individuals to whom the data pertains and to whom it will be applied.[127]

The analysis of fairness needs to protect against unseemly or risky actions but also to enhance beneficial opportunities. There are risks related to being too reticent with data. Human rights speak to shared benefits of technology and broader opportunities related to employment, health and safety. Pre-empting such opportunities is also a fairness issue. Indeed, a benefit of value to the organisation may also lead to a value to the public. If organisations do not do the analytics, then society will not benefit, but if the analytics are done, then the EU ICDIA needs to evaluate whether a benefit actually flows to the individual.

In considering the value of being fair, organisations should take steps to balance individual rights in a manner that gives weight to the interests of other parties but recognizes that not all interests have the same weight and that the rights of those individuals who will be impacted by the analysis have priority.[128] Fairness is a component of determining whether the processing of data is in compliance with the data processing principles and whether a legal basis to process is appropriate.[129] The existence of a legitimate interest needs careful assessment including whether a data subject can expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.[130] Results should not be gamed to favor the data users.

Conclusion

This paper has introduced the EU ICDIA, a framework for trusted accountability when organisations are using legitimate interest as the legal basis for processing data in innovative ways, particularly when using advanced analytics, and/or conducting DPIAs for high-risk processing, including big data analytics and other data intensive processing. The EU ICDIA protects fundamental rights and interests beyond just autonomy. In order to look at a full range of interests, a set of values to measure against that go beyond fair information practice principles is needed. The five core values serve this purpose. It also is necessary to define the desired outcome of the EU ICDIA, and the concept of legal, fair and just is a useful approximation of outcomes that are seen as responsible.

The EU ICDIA helps organisations determine whether its processing is legal, fair and just and demonstrate how this determination was reached. If done correctly, the EU ICDIA also enables transparency within the organization, to data subjects, to society, and to regulators.

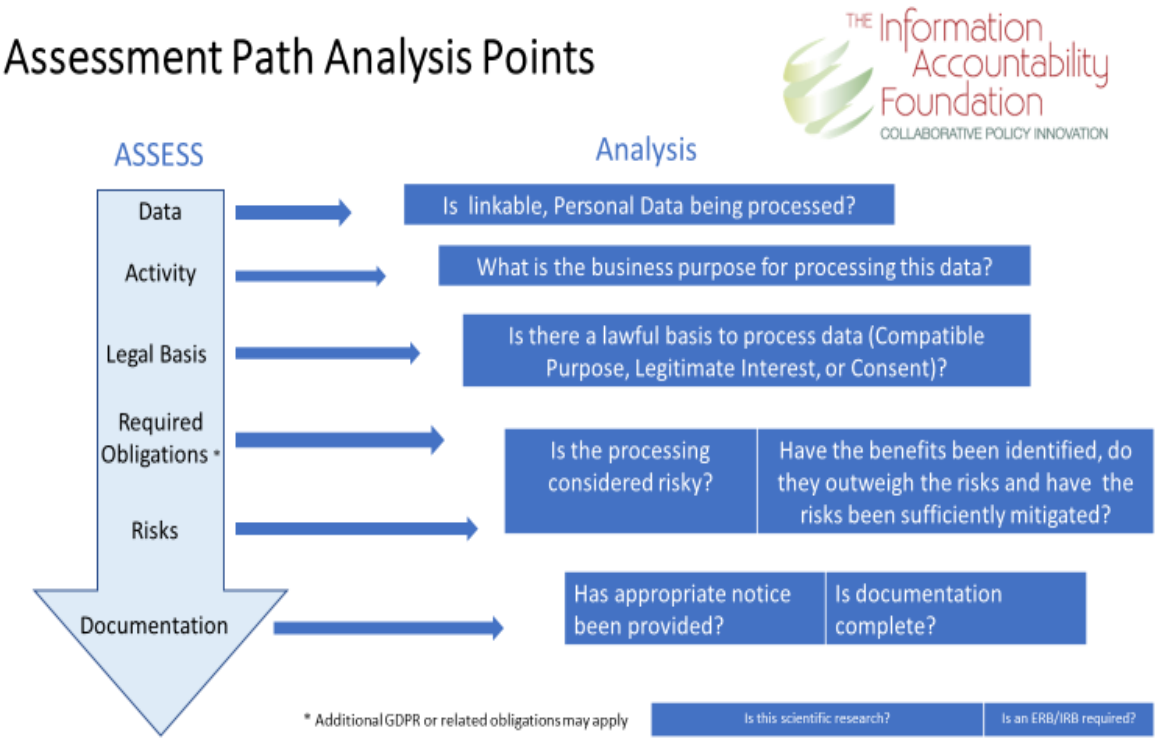
The GDPR will strengthen consumer trust in the European digital economy and make it easier for companies to carry out their business activities in the EU. The requirements of legitimate interest

[127] GDPR Article 5(1) (a) ("Personal Data shall be: Processed lawfully, fairly and in a transparent manner in relation to the data subject.")
[128] WP 217 at 23
[129] See text at notes 12-27 *supra*
[130] GDPR Recital 47

assessments and DPIAs overlap, and therefore, in practice, organisations will want to implement these assessments in an integrated manner. This paper also shows how the requirements for these

assessments are similar and therefore, how they can be conducted either separately or when appropriate incorporated together. When conducted in an integrated manner, the EU ICDIA will be more efficient and requirements will not be unnecessarily repeated, thus achieving the strengthening of consumer trust and making it easier for organisations to carry out their business activities.

III. EU INTEGRATED DECISON/EVALUATION SUMMARY



IV. EU INTEGRATED COMPREHENSIVE DATA IMPACT ASSESSMENT

Organisations that base processing on legitimate interests must conduct a balancing assessment that weighs the benefits to all stakeholders from the processing against the risks to all stakeholders. Where the risks outweigh the benefits, and the risks may be mitigated, the assessment enables documentation of the safeguards that further reduce the risks of the processing, making the processing acceptable. When an organisation needs to determine whether a data protection impact assessment (DPIA) is required for any activity or processing, if high risk processing is involved, the DPIA documents the safeguards and other benefits that reduce the inherent risks of the processing. Since a risk/benefit analysis is common to both assessments, and compliance with the data processing principles and the necessity and proportionality obligations is required for both assessments, many organisations will conduct these assessments in an integrated manner. As a result, The Information Accountability Foundation (IAF), based on a technology assisted assessment process developed by TrustArc, has developed the EU integrated comprehensive data impact assessment (EU ICDIA). Integration of these two assessments has the potential to strengthen individual trust in the robust use of data. The EU ICDIA makes it easier for business to conduct these assessments.

The EU ICDIA is a framework for trusted accountability when organisations are using legitimate interest as the legal basis for processing data in innovative ways, particularly when using advanced analytics, and/or conducting DPIAs for high-risk processing, including big data analytics and other data intensive processing. EU ICDIAs advance fundamental rights and interests beyond just autonomy. In order to look at a full range of interests, a set of values to measure against that go beyond fair information practice principles is needed. These values, (i) Beneficial, (ii) Progressive, Necessary and Proportional, (iii) Sustainable, (iv) Respectful of Obligations, and (v) Fairness – Reasonable Expectations of the Data Subject,[131] are interwoven throughout the EU ICDIA. It also is necessary to define the desired outcome of the EU ICDIA, and the concept of legal, fair and just is a useful approximation of outcomes that are seen as responsible.

The EU ICDIA helps an organization determine whether its processing is legal, fair and just and demonstrate how that determination was reached. If done correctly, the EU ICDIA also enables transparency within the organization, to data subjects, to society and to regulators.

The EU CDIA is comprised of four parts:

A. Data Governance and Accountability
B. Risks, Impacts and Benefits
C. Further Mitigating Controls and Other Safeguards
D. Outcomes – Reporting

Included within these four Parts are elements specific to data analytics. Each Part contains three columns: Questions, Factors/Responses to Consider and GDPR/Other References. To conduct a EU ICDIA, elements that comprise both a legitimate interest assessment and a DPIA are included. As such,

[131] See the paper, GDPR Integrated Risk Assessments – DPIAs and Legitimate Interests – To Isolate Risks and Benefits and Demonstrate Compliance, accompanying this EU ICDIA for a discussion of these values.

the EU ICDIA serves as a guidance framework that demonstrates how all related components could be integrated together

This guidance is not constructed so that it may be implemented as drafted, but rather it is meant as advice and direction and as a demonstration vehicle. It is not expected that this guidance will be the assessment itself. Rather, the EU ICDIA is proposed as a structure for organisations to use in developing their own assessment. This guidance is overly detailed so that decision makers will have options in developing their own assessment, and it is designed so that an organisation may create its own assessment to fit and accommodate its maturity, including its scope, size and scale of data processing, and specific structure, sector, and industry. It is not expected that every question will be asked by any given organisation.

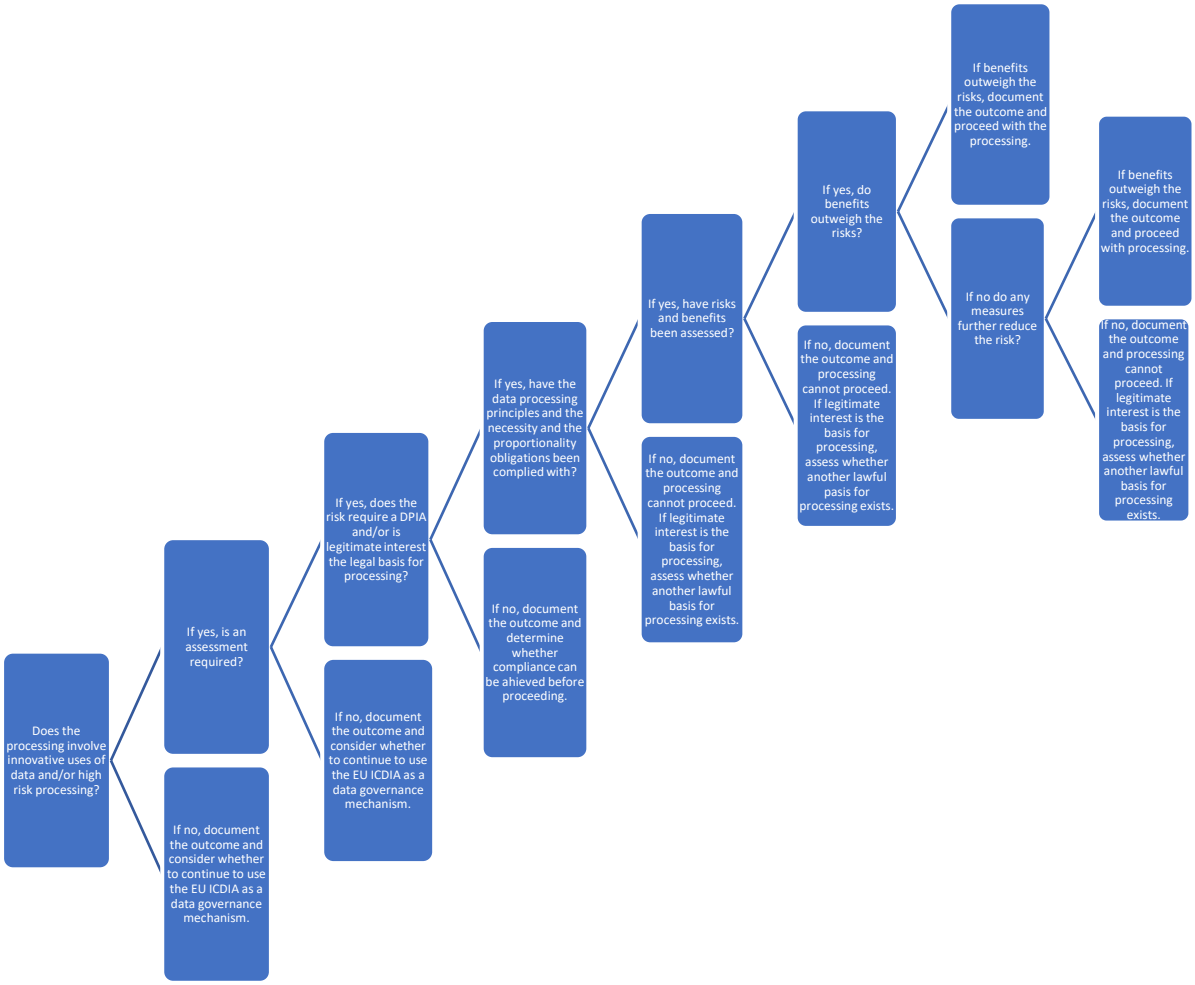
The EU ICDIA may be used in conjunction with an organisation's personal data processing inventory or associated records for purposes of GDPR compliance. Organisations may incorporate the EU ICDIA in whole or in part into their own unique processes and programs and may use it as a triage process to determine the questions that may be appropriate to ask considering their own circumstances and the level of assessment necessary. For example, if the activity in question is only minimally changed from the past, no assessment may be necessary. This approach will be particularly relevant to processing that may have already undergone a legitimate interest assessment or DPIA. If data is being used in a manner that is crystal clear from privacy notices and context, then a complete assessment may be unnecessary. If the level of risk is low, then it may be unnecessary to consider all Parts, and minimal documentation may be all that is necessary.

When processing does not involve innovative uses of data and/or high risk processing or such processing is involved but an assessment is not required, the EU ICDIA may be used as a data governance mechanism. Likewise, if during the assessment, it is determined that the data processing principles and/or the necessity and proportionality obligations have not been complied with, the EU ICDIA may function as a data governance mechanism. At any of these points, early exit from the EU ICDIA may be appropriate. (See the EU ICDIA process flow on page 24 which illustrates some but not all scenarios.)

Since an Outcomes Summary and Analysis Report may be generated upon completion of the assessment (Part D), if the processing does not involve high risk or legitimate interest processing, the assessment may still be used to document that the activity is compliant with the GDPR. The types and number of questions completed may be scaled according to the purpose of the activity and the relative level of the risk. The degree of documentation needed may be dependent upon the level of risk involved. In addition, all the reports in Part D may serve as describable output to fulfill the GDPR documentation requirements.

EU ICDIA PROCESS FLOW

(illustrating some but not all scenarios)



Part A: Data Governance and Accountability		
The questions in this Part relate to both legitimate interest assessments and DPIAs.		
Section 1. Organizational Governance and Accountability		
The questions in this Section are intended to identify the individuals who are responsible and accountable for the activity.		
Questions	Factors/Responses to Consider	GDPR/Other References
Identify the organization and the ultimately accountable decision-maker for the activity.	Day-to-day management of the activity Data analysis Third party management Technology support and compliance	
Identify other stakeholders responsible for other parts of the activity.		
Section 2. Purpose		
The questions in this Section are intended to identify the purpose and intended outcomes of the activity (these purposes may be imported in from a data governance or inventory management application)		
Questions	Factors/Responses to Consider	GDPR/Other References
What is the business need that prompted this activity or the intended primary purpose of the processing (i.e., the main reason your organisation plans to collect, use and/or disclose the data)?		GDPR Article 5(1)(b) Purpose Limitation WP 203
Identify any other business needs for this data?		GDPR Article 5(1)(b) Purpose Limitation WP 203
How does the purpose of the activity fit within the organization's current business strategy?		GDPR Article 5(1)(b) Purpose Limitation
How does the purpose of the activity align with the values of the organization?	Values can be found in the organisations's mission statement, code of ethics or corporate social responsibility goals	GDPR Article 5(1)(b) Purpose Limitation
How does the purpose of the activity fit within the values of society?		GDPR Article 5(1)(b) Purpose Limitation

Does the activity involve data analytics?
If yes,
• Is the purpose of the activity to think with data or to act with data?
• If generate insights,
  ○ how were the potential insights derived?
  ○ will the activity expand on insights from a previous activity?
  ○ if the activity expands upon a previous activity, could the activity be considered a compatible purpose?
  ○ how might the potential insights be used?
  ○ are the uses of the potential insights internal to the organization only or will they be shared with others?
  ○ how long might the documentation regarding the potential insights endure?
  ○ could the potential insights become less useful or valuable over time?
  ○ are the potential insights repeatable?
  ○ for how long are the potential insights repeatable?
  ○ could the application of the potential insights impact behavior in a manner that could reduce the predictive value of the insights over time?
• Are the potential insights reliable enough for the
		GDPR Article 5(1)(b)
		GDPR Article 4(4)
		Definition Profiling
		GDPR Article 5(1)(c) Data
		Minimisation
		GDPR Article 5(1)(d)
		Accuracy
		GDPR Recital 75

purposes of the activity? • Is there a less data-invasive way to obtain the potential insights? • Is it foreseeable that the potential insights might seem inappropriate or discriminatory or might be considered offensive causing distress or humiliation?		
Have the specific data types needed for the purposes of the activity been defined?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 5(1)(c) Principles relating to processing of personal data

Are data processed in connection with the activity solely for the purposes identified? If the answer is "No" or "Don't Know",
 	
• Are data processed for scientific or historical research purposes or statistical purposes?
  ○ If for scientific research,
  ▪ Is the data processed for the purpose of technological development research or fundamental research (systematic investigation designed to increase knowledge)?
  ▪ Is the data that will be processed sensitive?
  ▪ Will the results of the activity be published in a journal or other publication?
  ○ Does the scientific research require
	Explanations can be provided by adding comments or attaching documentation.
	
	A "compatible purpose" related or linked to the purpose for which the data were originally collected, and is consistent with the context in which the data was collected. The proposed compatible purpose will, in particular, meet the reasonable expectations of individuals, given the nature and sensitivity of the data, and the existence of appropriate information safeguards.
	
	An "incompatible purpose" does not link to the purpose for which the data were collected, does not align with the context in which the data was collected, in particular, the reasonable expectations of individuals given the nature of the data, and may have unintended or adverse consequences for the individuals about whom the data are processed.
		GDPR Article 5(1)(b) Purpose limitation.
		
		GDPR Article 6(4) Lawfulness of processing
		
		GDPR Article 89(1) Scientific research

review by a data review board? ○ Does the scientific research require review by the Institutional Review Board? ▪ Will the activity be conducted by an academic institution working with the company? ▪ Is the processing potentially intended to be used as part of a submission to a medical regulatory agency for product approval? • Are the data processed for other compatible purposes? • Are the data processed for other incompatible purposes?		
Section 3. Data		
The questions in this Section are intended to identify the types of data needed for the activity (these data elements may be imported in from a data governance or inventory management application).		
Questions	Factors/Responses to Consider	GDPR/Other References
What data elements related to individuals does the activity involve?		GDPR Article 4(1) Definitions "personal data" GDPR Article 9 Processing of special categories of personal data.
List the other data elements related to an individual that are processed in connection with the activity		GDPR Article 4(1) Definitions "personal data" GDPR Article 9 Processing of special categories of personal data
Are the data reasonably linkable to a particular individual?		GDPR Article 4(1) Definitions "personal data"
Section 4. Data Sources, Origins and Characteristics		

The questions in this Section identify the sources and origins of the data to be used in the activity. Data accuracy may be directly related to how the data was sourced. Data directly observed may be more precise than data inferred from an algorithm. Data directly observed may be more accurate than data volunteered by individuals. The origins of the data should be considered. See The Origins of Personal Data and Its Implications for Governance*. Mitigating controls and safeguards should be implemented accordingly.*		
Questions	Factors/Responses to Consider	GDPR/Other References
Are data collected directly from the individuals to whom the data relate?		
Are data collected passively (e.g. through online tracking technologies such as cookies or web beacons, sensors or surveillance cameras)?		
Are data obtained from or provided by third parties? If Yes, list the third parties.		
Are there data elements to be used that are the product of a probability-based process, such as a score?		
Are data collected, generated, sourced or used in other ways? • Are data created through statistical analysis or calculations? • Are the data scraped from the web? • Are data obtained from public sources? • Are data provided by a third-party data aggregator or data broker? • Are the data generated by sensors (e.g. in a connected device)? • Are the data observed in some other fashion not otherwise described (e.g. through a camera or some other mechanism that may not be under the control of the individual being observed)? • Are the data derived from other data (e.g. through some form of transformation or manipulation)? • Are the data inferred from		

some form of analysis? • Are the data obtained from social media platforms? • Are the data structured or unstructured or both? Is the personal data that is collected and processed limited to the information necessary, relevant and proportionate to the purposes of the activity?		
Does data exist elsewhere in the organization?		
Section 5. Data Integrity and Quality		
The questions in this Section examine and assess the safeguards for keeping data sufficiently accurate, complete, relevant, and current consistent with its intended use.. All controls identified as mitigating controls to a particular risk are applied to inherent risk or benefit adjusted inherent risk and used to determine residual risk.		
Questions	Factors/Responses to Consider	GDPR/Other References
Are mechanisms in place to ensure that the data are accurate, and where necessary, kept up to date?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 5(1)(d) Principles relating to processing of personal data - accuracy
Data preparation: Do the mechanisms include processes: • to put the data in a consistent format? • to address any impact of time on the data? • for evaluating the data before consolidating it? • to address any changes to the data as they are used, analyzed or otherwise processed? • to address any changes to the identifiability of the data as they are used, analyzed or otherwise processed? • for managing further synthesis of the data, including deriving data elements from various source elements, where necessary to the activity?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 5(1)(d) Principles relating to processing of personal data - accuracy
Are mechanisms in place to ensure that any inaccurate data are rectified or erased without delay?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 5(1)(d) Principles relating to processing of personal data – accuracy
Accuracy: Do the mechanisms include:	Explanations can be provided by adding comments or attaching	GDPR Article 5(1)(d) Principles relating to processing of personal

• processes for evaluating whether the age of the data affects its accuracy? • processes for determining whether the predictive level of any inferred data is and remains accurate? • processes for determining whether the predictive level of any inferred data is and remains accurate? • Evaluation of any steps that could be taken to protect individuals (such as pseudonymization) without impacting the accuracy of the data?	documentation.	data - accuracy
Section 6. Data Subjects		
The questions in this Section identify the types of individuals about whom data will be processed in connection with the activity. Certain types of data subjects may be more significantly impacted by the data processing. The responses in this Section may contribute to the analysis of risk severity later in this assessment. (These data subjects may be imported in from a data governance or inventory management application)		
Questions	Factors/Responses to Consider	GDPR/Other References
Identify the types of individuals about whom data are processed in connection with this activity.		GDPR Article 30 (1)(c) Records of processing activities
Section 7. Transparency		
The questions in this Section examine and assess the mechanisms for informing individuals about the ways in which data about them are processed and how to exercise their data-related rights.		
Questions	Factors/Responses to Consider	GDPR/Other References
Does the activity include mechanisms for ensuring that information about data processing and individuals rights is provided before information is collected from individuals, at the time of collection, or as soon as practicable thereafter?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 5(1)(a) Principles relating to processing of personal data - lawfulness, fairness and transparency.
Does the information provided to individuals about whom data are processed in connection with the activity include in a privacy statement, layered notice, informed consent form or other form of notice all of the	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 13(1), (2) (4). Information to be provided where personal data are collected from the data subject. GDPR Article 14(1), (2), (4). Information to be provided where

following? • The identity and contact details of the controller and, where applicable, of the controller's representative • The contact details of the data protection officer, where applicable • The purposes of the processing for which the personal data are intended as well as the legal basis for the processing • Where the processing is based on legitimate interests, the legitimate interests pursued by the controller or by a third party • Where the data are collected from a source other than the individual, the categories of personal data processed, the sources of the data and, is applicable, whether it came from publicly accessible sources • The recipients or categories of recipients of the personal data, if any • If data will be transferred to a third country, the legal mechanism or basis for the transfer and how to obtain more information, where applicable • The retention period for the personal data or the criteria for determination of the retention period • The applicable individual rights and how to exercise them • Where processing is based on consent, the right to withdraw consent at any time without affecting the lawfulness of the processing based on such consent before withdrawal • The right to lodge a complaint with a data protection authority • Where the data are collected from the individual, whether		personal data have not been obtained from the data subject.

there is a legal or contractual requirement for the data and the possible consequences if the data are not provided • Where applicable, that automated decision-making, including profiling, is involved, meaningful information about the logic involved, and the potential significance and consequences of such processing for the individual If No, do the individuals already have the following information (e.g. was it previously provided or known to the individuals)?		
If the data are obtained from a source other than the individual, is the privacy notice and required information provided according to the earliest of the following times? • No later than one month after the data are obtained • At the time of first communication with the individual At the time of first disclosure to another recipient	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 14(3) Information to be provided where personal data have not been obtained from the data subject.
If additional processing for new purposes is planned in connection with the activity, is an updated privacy notice describing those purposes and any additions to the information previously provided made available to the individuals?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 13(3) Information to be provided where personal data are collected from the data subject. GDPR Article 14(4) Information to be provided where personal data have not been obtained from the data subject.
Is the privacy notice provided in connection with the activity displayed in a clear and conspicuous manner?	Explanations can be provided by adding comments or attaching documentation.	
If a personal data breach occurs in connection with the activity, and the breach is likely to result in high risk to the rights and freedoms of individuals, is a mechanism in place to ensure that the notification to individuals describes	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 34 Communication of a personal data breach to the data subject

at least the following in clear and plain language? • The nature of the personal data breach • The name and contact details of the DPO or other contact point where additional information can be obtained • The likely consequences of the personal data breach Measures taken to address and, where appropriate, mitigate the possible adverse effects of the breach		
Section 8. Supporting Technologies and Third Parties and Other Data Recipients		
The questions in this Section identify the involvement of technologies, third parties and data recipients in the activity. Involvement of certain technologies and third parties may affect the risk of the data processing. The responses in this Section may contribute to the analysis of risk likelihood later in this assessment. (These inputs may be imported in from a data governance or inventory management application)		
Questions	Factors/Responses to Consider	GDPR/Other References
Identify any applications, systems or other technologies used as part of or in support of the activity?	If a third party supports the application, system or technology, provide the name of the third party and country in which the technology is located as well.	GDPR Article 30 (1) Records of processing activities
Identify any third party organizations or individuals (and their relevant roles) that have access to the data in connection with the activity?	Vendors or business partners	GDPR Article 30 (1) Records of processing activities
Identify any other recipients, or categories of recipients, of the data who will have access to the data?		GDPR Article 30 (1) Records of processing activities
Section 9. Lawfulness of Processing		
The questions in this Section examine and assess the basis for the lawful processing of personal data, focusing on the most common: consent and legitimate interest		
Questions	Factors/Responses to Consider	GDPR/Other References

Which mechanism does the activity rely on as its legal basis for processing?	This question is intended to identify the mechanism that will be relied upon to make the processing lawful: consent, contract, legal obligation, vital interest, public task, legitimate interest	GDPR Article 6(1) Lawfulness of Processing
If "Legitimate Interest" is the legal basis for processing, • is the purpose for the processing aligned with the purpose articulated in Section 2 above? • do the benefits of the activity outweigh the inherent risk? If yes, go to Sections 9 and 10 below.		GDPR Recitals 47-49 GDPR Article 6(1) Lawfulness of Processing WP 217
If "Consent" is the legal basis for processing, • is the form of consent presented to the individual clear, written in plain language, conspicuous and presented in a manner that is clearly distinguishable from other information presented to the individual? • are there conditions that may conflict with consent being freely given (e.g. is the performance of a contract conditioned on the individual providing consent for data processing that is not necessary for the performance of that contract)? • is evidence of individual consent able to be demonstrated upon request? • are individuals informed of their right to withdraw consent at any time? If yes, early exit from the EU CDIA.	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 6 Lawfulness of processing. GDPR Article 4(11) Definitions – consent GDPR Article 7 Conditions for consent
If data are collected from children below the age of 16 (or a lower age where permitted by Union or Member State law, but in no case lower than the age of 13),	Explanations can be provided by adding comments or attaching documentation.	Article 8(1), (2). Conditions applicable to child's consent in relation to information society services

• has verifiable parental consent been obtained? If yes, early exit from the EU CDIA.		

Part B: Risks, Impacts and Benefits: Legitimate Interests and DPIA Balancing

The questions in Sections 10 - 13 relate to DPIAs. If legitimate interest is the basis of processing, only the questions in Sections 11 – 13 apply.

Section 10. High Risk Processing

The questions in this Section are intended to enable a determination of whether a DPIA is required under the GDPR.

Questions	Factors/Responses to Consider	GDPR/Other References
Does the activity involving any high-risk processing? If yes, and legitimate interest is not the basis of processing, go to Part C.	Evaluation or Scoring Automated-Decision Making with Legal or Similar Significant Effect Systematic Monitoring Sensitive Data Data Processed on a Large Scale Datasets that have been Matched or Combined Data Concerning Vulnerable Subjects Innovative Use or Applying Technological or Organisational Solutions Data Transfer Across Borders Outside European Union (EU) Interference with Rights or Opportunities Other Likely High Risks to the Fundamental Rights or Freedoms of Individuals None	The purpose of this question is to determine whether the activity is likely to result in a high risk to the rights and freedoms of individuals which requires a Data Protection Impact Assessment (DPIA) under GDPR Article 35 GDPR Recital 75 WP 248
Does the activity involve any other potentially high risk factors or attributes? If yes, and legitimate interest is not the basis of processing, go to Part C.	Data use out of context (beyond reasonable expectations) Data use beyond the effective durability of the insights that can be derived from the data	

Section 11. Value and Benefit of the Processing

The questions in this Section are intended to identify the value of the activity to the organisation, to society and to individuals.

Questions	Factors/Responses to Consider	GDPR/Other References

Identify the benefit (beneficial impact) to the organisation of conducting the activity (i.e., what value does the organisation expect to achieve?)	Increased revenue Lower costs Improved profitability Greater market share Enhanced employee satisfaction, engagement and productivity Enhanced customer relationship Enhanced or maintenance of brand or reputation Assurance of compliance Limitation of legal liability Fraud prevention Crime prevention Enhanced or maintenance of physical security Enhanced or maintenance of cyber security New or improved products or services Improved customer service Direct Marketing Group of undertakings data transfers Network and information security Other	GDPR Article 6(1)(f) Lawfulness of processing WP 217
Identify the benefit (beneficial impact) of the organisation conducting the activity to the community or society.	Better health care Better health outcomes Lower cost health care Improved education Environmental enhancements Water conservation Energy cost reduction Infrastructure enhancements Economic improvement More accessible/usable technology Increased job opportunities Protection of reasonable expectation of privacy, including anonymity Protection of freedom of religion, thought and speech Protection of prohibition against discrimination on the basis of race, national or ethnic origin, colour, region, age, sex, sexual orientation, marital status, disability or genetics Other	GDPR Article 6(1)(f) Lawfulness of processing WP 217

Identify the benefit (beneficial impact) of the activity to the individuals' whose data are processed.	More objective or safer interactions Better product selection and utilisation Better access to new products and services Significant discounts Improved service Improved ease of use Engaged consumers/customers/employees More convenience Appropriately linked to other choices, etc. Anticipating or meeting of a need Exercise of self-determination Public sector access Anonymous transportation Improved health and well being Improved financial condition Lower cost alternatives Increased options Other	GDPR Article 6(1)(f) Lawfulness of processing WP 217
Section 12. Inherent Risk Assessment		
The questions in this Section are for the purpose of determining the risks to interests and fundamental rights of the individual and to society.		
Questions	Factors/Responses to Consider	GDPR Reference
Identify any factors present that are more likely to increase the severity or impact of the risk for individuals.	Physical harm Financial harm Harm due to crime or terrorism Reduced health and well-being Damage to reputation Embarrassment Shock or surprise Inappropriate discrimination Inappropriate access to or misuse of data, including sensitive or special categories of data and directly identifiable data Manipulation of needs (i.e. creation of a need where one previously did not exist) Data that are the product of a probability-based process, such as a score Data subjects who may be in a more	GDPR Recital 75

	vulnerable position than the organisation processing the data Larger volume processing (versus a small scale pilot) Incidental findings None	
Identify any factors present that are more likely to increase the severity or impact of the risk for society as a whole.	See Section 10 above Discrimination Differential impact Exclusion Security Breach	
Identify any factors present that are more likely to increase the likelihood or probability of the risk.	Resource constraints (e.g. financial, human) Third parties involved in data processing Larger number of parties involved in data processing Lower organizational privacy, compliance or data governance maturity None	GDPR Recital 75 GDPR Article 35
Section 13. Inherent Risk-Benefits		
The questions in this Section determine whether processing may proceed or whether further risk reduction measures are necessary. If processing may proceed, that decision should be documented through the reports produced in Part D.		
Questions	Factors/Responses to Consider	GDPR References
Do the benefits outweigh the risks?		WP 217
If yes, proceed to Part D to document the outcome		GDPR Recital 75
If no, proceed to Part C.		GDPR Article 35
Part C: Further Mitigating Controls and Other Safeguards		
The questions in this Part apply if after the risk/benefit test in Part B, risks outweigh benefits.		

Section 14. Data Necessity: Data minimization, Data protection by design, Data protection by default		
The questions in this Section examine and assess further safeguards for enabling data value to be optimized. Anonymization, de-identification, pseudonymization, and coding should be leveraged to mitigate data storage-related risks.		
Questions	Factors/Responses to Consider	GDPR/Other References
To minimize the likelihood that they can be used to identify an individual, have the data been: • aggregated? • pseudonymized?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 25(1) Data protection by design and by default.
Do the data include a code or other data element(s) that allow the data to be combined with other data to make it re-identifiable?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 4(5) Definitions. Pseudonymisation
Have technical and organizational measures been implemented to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 25.2 Data protection by design and by default
Section 15: Retention and Disposal		
The questions in this Section examine and assess the safeguards for ensuring that data is used solely for purposes that are relevant to and compatible with the purposes for which it was collected.		
Questions	Factors/Responses to Consider	GDPR/Other References
Has a retention period been defined for the data processed in connection with the activity? • If Yes, has the retention period been documented in the records of processing activities for GDPR Article 30 purposes? • If No, have the criteria to determine how long the data may need to be retained been documented in the records of processing activities for GDPR Article 30 purposes?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 5(1)(e) Principles relating to processing of personal data - storage limitation GDPR Articles 13(2)(a), 14(2)(a), 15(1)(d), 30(1)(f) Retention periods
Section 16. Disclosure to Third Parties and Onward Transfer		
The questions in this Section examine and assess the safeguards for preserving the standards and protections for data when it is transferred to third-parties and/or across country borders. All controls identified as mitigating controls to a		

particular risk are applied to inherent risk or benefit adjusted inherent risk and used to determine residual risk.		
Questions	Factors/Responses to Consider	GDPR/Other References
If third parties (e.g. vendors) process data in support of the activity, have the privacy and security practices of those third parties been evaluated to ensure that they are able to comply with the standards and controls required by this assessment and applicable laws to protect the data and the rights of individuals?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 28(1) Processor
Are written (or electronic) contracts in place with all third parties (e.g. vendors and business partners) that require, at a minimum, all of the data protection standards in GDPR Articles 28(3), (4), (9)?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 28(3), (4), (9) Processor
If data are transferred to a third country, have any applicable requirements for international data transfer been met?	Explanations can be provided by adding comments or attaching documentation. Countries that restrict cross-border data transfer are: European Economic Area (includes EU): Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lichtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, UK. Other Europe: Azerbaijan, Russia, Switzerland, Ukraine. Middle East: Dubai Financial Centre, Israel, Qatar Financial Centre, Turkey. Africa: Angola, Benin, Burkina Faso, Cape Verde, Cote D'Ivoire, Gabon, Madagascar, Mali, Mauritius, Morocco, Senegal, South Africa, Tunisia. Asia Pacific: Australia, China (sectoral), Hong Kong (not yet effective), India, Japan, Malaysia, Singapore, South Korea, Taiwan. Americas: Argentina,	GDPR Article 44 General principles for transfers

	Canada (agreements for data processors and onward transfers), Brazil (Internet only), Colombia, Peru, Uruguay.	
If data are transferred internationally inside of the organisation (e.g. to subsidiaries and affiliates globally), what data transfer mechanisms are used?	Binding corporate rules EU-US Privacy Shield (EU to US organizations only) Swiss-US Privacy Shield (Swiss to US organizations only) APEC Cross Border Privacy Rules Standard Contractual Clauses Individual consent to the transfer Contracts between controller and data subject Contracts in the interest of the data subject Public interest - the transfer is necessary for important reasons of public interest Legal claims - the transfer is necessary for the establishment, exercise or defence of legal claims Vital interests - the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; Other (describe) Don't know	GDPR Article 44 - General principle for transfers GDPR Article 45 - Transfers on the basis of an adequacy decision GDPR Article 46 - Transfers subject to appropriate safeguards GDPR Article 47 - Binding corporate rules GDPR Article 48 - Transfers or disclosures not authorized by Union law GDPR Article 49 - Derogations for specific situations GDPR Article 50 - International cooperation for the protection of personal data
If data are transferred internationally to other organisations (e.g. to suppliers in other countries), what data transfer mechanisms are used?	Binding corporate rules EU-US Privacy Shield (EU to US organizations only) Swiss-US Privacy Shield (Swiss to US organizations only) APEC Cross Border Privacy Rules Standard Contractual Clauses Individual consent to the transfer Contracts between controller and data subject Contracts in the interest of the data subject Public interest - the transfer is necessary for important reasons of public interest Legal claims - the transfer is necessary for the establishment, exercise or	GDPR Article 44 - General principle for transfers GDPR Article 45 - Transfers on the basis of an adequacy decision GDPR Article 46 - Transfers subject to appropriate safeguards GDPR Article 47 - Binding corporate rules GDPR Article 48 - Transfers or disclosures not authorized by Union law GDPR Article 49 - Derogations for specific situations GDPR Article 50 - International cooperation for the protection of personal data

	defence of legal claims Vital interests - the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; Other (describe) Don't know	
If transfers are made to a third country, has the identification of the third country been documented in the records of processing activities for GDPR Article 30 purposes?	Explanations can be provided by adding comments or attaching documentation	GDPR Article 30(1)(e) Records of processing activities
Section 17. Access and Individual Rights		
The questions in this Section examine and assess the safeguards for enabling individuals to access information about themselves, to amend, correct, and, as appropriate, delete information that is inaccurate, incomplete, or outdated. It specifically addresses the following individual rights under the GDPR: access, rectification, erasure, restriction, data portability and objection (including the right not to be subject to a decision based solely on automated data processing, including profiling).		
Questions	Factors/Responses to Consider	GDPR/Other References
Access: Is a mechanism in place for individuals to request access to information about the personal data processing regarding him or her in connection with the activity as well as the following information? • The purposes of the processing • The categories of personal data concerned • The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations • Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period • The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 15(1), (2). Right of access by the data subject

concerning the data subject or to object to such processing • The right to lodge a complaint with a supervisory authority • Where the personal data are not collected from the data subject, any available information as to their source • The existence of automated decision-making, including profiling, and in those cases, meaningful information about the logic involved • If personal data are transferred to a third country or to an international organization in the absence of an adequacy decision, the safeguards in place for the transfer		
Access: Is the access mechanism available and able • to promptly deliver the information to an authenticated authorized requestor online or other commonly used electronic form? • to provide to individuals, at no cost to the individuals, a copy of the personal data about them that is processed in connection with the activity?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 15(3) Right of access by data subject
Rectification: Is a mechanism in place to enable individuals to rectify inaccurate or incomplete personal data processed by the technology, process, or activity? If Yes, • is a mechanism in place to communicate rectification of personal data to any recipients of the personal data to whom the personal data have been disclosed, including to any third party data processors? • is a mechanism in place to inform data subjects, upon request, of the recipients of personal data about them?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 16 Right to rectification GDPR Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing
Erasure ("right to be forgotten"): Does one or more of the following conditions		GDPR Article 17(1) Right to erasure

apply to the activity? • The data no longer are necessary for the defined business purposes for which they were collected or otherwise processed • The data subject withdraws his or her consent and there is no other legal basis for the processing • The data subject objects to the processing and there are no overriding legitimate grounds for the processing or, the processing is for direct marketing purposes and the data subject objects • The data have been processed without a lawful basis • An obligation under the applicable laws [of the country or the EU] requires deletion of the data • The data have been collected from a child in connection with a website, mobile app or other online service		(right to be forgotten)
Erasure ("right to be forgotten"): Does one or more of the following exceptions apply to the activity? The ongoing processing is necessary for: • Exercising the right of freedom of expression and information • Compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller • Reasons of public interest in the area of public health • Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes where the right to erasure (the right to be		GDPR Article 17(3) Right to erasure (right to be forgotten)

forgotten) is likely to render impossible or seriously impair the achievement of the objectives of that processing • The establishment, exercise or defense of legal claims		
If the answer to the first “Erasure” question is “Yes,” and the answer to the second “Erasure” question is “No,” is a mechanism in place to delete the data upon request from an individual to whom those data relate, including any links to, or copy or replication of, those personal data?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 17(1), (3) Right to erasure (right to be forgotten)
Erasure (“right to be forgotten”): Does the activity involve making personal data public (e.g. through display of search engine results)? If Yes, is a mechanism in place to inform others who may have access to that data that the individual has requested deletion of the data, including any links to, or copy or replication of, those personal data?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 17(2) Right to erasure (right to be forgotten)
Erasure ("right to be forgotten"): Is a mechanism in place to communicate obligations to delete personal data processing to any recipients of the personal data to whom the personal data have been disclosed, including to any third party data processors?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing
Restrictions: Does one or more of the following conditions apply to the activity? • Accuracy: The data subject has contested the accuracy of the personal data and the data controller is in the process of verifying the accuracy of the personal data • Unlawful: The processing is unlawful and the data subject has requested restriction of the data use rather than erasure of the data • Legal Claims: The data	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 18(1), (2) Right to restriction of processing

controller no longer needs the data for the activity or any legitimate further processing; however, the data subject needs them for the establishment, exercise or defense of legal claims • Objection: The data subject has objected to the data processing and the data controller is in the process of determining whether compelling legitimate grounds for the processing override the interests, rights and freedoms of the data subject		
If "Yes," Is a mechanism in place to restrict processing of personal data, to inform the individual prior to lifting the restriction, and to ensure that, with the exception of storing those data, the processing occurs only as follows? • With the consent of the individual • For the establishment, exercise or defense of legal claims • For the protection of the rights of another natural or legal person For reasons of important public interest of the EU or and EU member		
Restrictions: Is a mechanism in place to communicate restrictions on personal data processing to any recipients of the personal data to whom the personal data have been disclosed, including to any third party data processors?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing.
Data Portability: Do both of the following conditions apply to the activity? • The processing is based on consent or on the determination that it is necessary for performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 20(1), (2) Right to data portability

into a contract; and • The processing is automated		
If Yes, is a mechanism in place to enable the data subject to receive and transmit to another data controller (including directly, where technically feasible) personal data, which has been provided by the data subject to the data controller, in a structured, commonly used and machine-readable format?		
Right to Object: Do both of the following conditions apply to the activity? • The processing is based on a determination that it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child, or on a determination that it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller • The controller has compelling legitimate grounds to process the data that override the interests, rights or freedoms of the individual, or the controller needs to process the data for the establishment, exercise or defense of legal claims	The balancing of interest assessment set forth in Article 21(1) is the part of the balancing of interest assessment under Articles 6(1) and 35(7).	GDPR Article 21(1) Right to object
Right to Object: Are the data processed for direct marketing purposes or for		GDPR Article 21(2), (3)

profiling related to direct marketing?		Right to object
Right to Object: Do both of the following conditions apply? • Are the data processed for scientific or historical research purposes or statistical purposes? • The processing is not necessary for an activity or task undertaken for public interest reasons?		GDPR Article 21(6) Right to object
If "No" to first and last "Right to Object" questions and "Yes" to "Direct Marketing" Question, is a mechanism in place to enable individuals to object to the processing of data about him or her? • If "Yes" and if the activity involves a web site, mobile app, or other online services, is the mechanism available online using automated means?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 21(5) Right to object
Right to Object to being subject to a decision based solely on automated processing: Does the activity involve decisions about individuals based solely on automated processing, including profiling, such as calculation of a score or ranking?		GDPR Article 22(1) Automated individual decision-making, including profiling
Right to Object - Automated Decision-Making, including Profiling: Do any of the following conditions apply to the activity? • The automated decision is based on the explicit consent of the individual • The automated decision is necessary for entering into, or performance of, a contract between the individual and the data controller • The automated decision is authorized by Union or Member State law, which applies to the data controller		GDPR Article 22(2) Automated individual decision-making, including profiling

and which also specifies appropriate mechanisms for safeguarding the individual's rights, freedoms and legitimate interests		
If "Yes" to first and "No" to second "Right to Object – Automated Decision-Making" questions, is a mechanism in place to enable the individual to object to an automated decision about him or her that would have a legal or other significant effect on him or her and does not involve any human intervention (e.g. automated online denial of credit or an opportunity to be considered for a job)?	Explanations can be provided by adding comments or attaching documentation.	
Right to Object - Automated Decision-Making, including Profiling: Does the decision-making involve sensitive data? If Yes, and the individual does not have the right not to be subject to a decision based solely on automated processing, including profiling, have both of the following conditions been met? • The processing is based on explicit consent or for reasons of substantial public interest, and • All of the necessary controls and safeguards set forth in this assessment are in the place.	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 22(4) Automated Individual decision-making including profiling
How effective are these controls and safeguards for reducing risk?		
Section 18. Security		
The questions in this Section examine and assess the safeguards for protecting data from loss, misuse and unauthorized access, disclosure, alteration or destruction.		
Questions	Factors/Responses to Consider	GDPR/Other References

Is there a comprehensive information security policy in place that applies to the activity?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 32(1) Security of processing
Are there authentication and access mechanisms in place for the activity (e.g. password protected access to systems containing personal data; two-factor authentication for access to systems containing sensitive data; smart card readers for physical access to data and systems containing personal data; based on roles and responsibilities for granting and terminating access to physical and electronic access to hardware, systems and data used in support of the activity)?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 32(1)(b) Security of processing
Are all personal data encrypted if and when: • they are transmitted in connection with the activity? • they are stored in connection with the activity?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 32(1)(a) Security of processing
If data are encrypted in connection with the activity, are key management procedures in place to protect keys and the metadata that the key management system supports?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 32(1)(a) Security of processing
Are removable media controls in place to prevent unauthorized dissemination of the data processing in connection with the activity?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 32(1)(b) Security of processing
Is there boundary protection (e.g. firewalls and intrusions detection) around the network(s) and system(s) used to process the data in connection with the activity?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 32(1)(b) Security of processing
Are incident detection, escalation and management procedures in place that apply to the activity?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 33 Notification of a personal data breach to the supervisory authority GDPR Article 34 Communication of a personal data breach to the data subject
Is a mechanism in place to determine	Explanations can be provided by	GDPR Article 33 Notification of a

whether an incident involves personal data in connection with the activity?	adding comments or attaching documentation.	personal data breach to the supervisory authority
Are processes in place for monitoring the systems used by the activity, including vulnerability scans?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 32(1)(d) Security of processing
Are data backup and disaster recovery procedures in place for the systems used by the activity?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 32(1)(c) Security of processing
Are data used in connection with the activity securely disposed of once the retention period for the activity has been reached or when otherwise no longer needed for the activity?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 32(1)(b) Security of processing
Have the identifiable data elements been replaced with a code or otherwise rendered in a form that cannot be attributed to a specific individual without the use of additional information that is kept separately and secured from unauthorized access (i.e., pseudonymized)?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 32(1)(a) Security of processing
Are there change control procedures in place for the applications and systems supporting the processing?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 32 (1)(d) Security of processing
Section 19. Monitoring and Assurance		
The questions in this Section examine and assess the mechanisms for evaluating and auditing effectiveness of controls and risk-mitigation measures in connection with the activity.		
Questions	Factors/Responses to Consider	GDPR/Other References
Have the risks and controls set forth in this assessment been reviewed by the accountable decision maker?	The accountable decision maker may be the data protection officer	GDPR Article 35(2) Data protection impact assessment. GDPR Article 39(1)(c) Tasks of the

		data protection officer
If the activity involves research or analytics using personal or pseudonymized data, have the risks and controls been reviewed by an ethical review board or similar oversight function with expertise in data ethics and/or human subjects research?		
Has the processing activity or its supporting technologies been certified as having appropriate safeguards in place?	Explanations can be provided by adding comments or attaching documentation.	GDPR Article 42(2) Certification
Section 20. Residual Risk Benefits		
The questions in this Section determine whether an activity can proceed or not. After than decision has been reached, it should be documented through the reports produced in Part D.		
Questions	Factors/Responses to Consider	GDPR References
Have the risks to individuals been further reduced?		WP 217
If yes, such that they are minimal in comparison to the benefits, then proceed to Part D to document the outcome.		Recital 75 Article 35
If no, the processing cannot proceed, and if legitimate interest if the Basis of processing, assess whether there is another lawful basis for processing. Then proceed to Part D to document the outcome.		
Part D: Outcomes and Reporting		
This Part produces reports based on the results from Parts A to C. All the reports in Part D may serve as describable output to fulfill the GDPR documentation requirements		
Reports generated are: • Mitigations and Safeguards Effectiveness Evaluation • Residual Risk Severity and Likelihood • Legitimate Interests Balancing Test Outcomes • Outcomes Summary and Analysis (Where residual risks are high, consultation of DPA and data subjects)		