



Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR

CIPL GDPR Interpretation and Implementation Project

21 December 2016

Table of Contents

1. Introduction and Recommendations	3
Part 1: The Risk-based Approach to Data Protection and Privacy	12
2. An Overview of the Risk-Based Approach to Data Protection and Privacy.....	12
2.1 Advantages of a Risk-Based Approach to Data Protection	12
3. What is “Risk”?	13
3.1 Defining Risk	13
3.2 Identifying the Elements of Risk (risky processing activities, threats and possible harms)	14
4. “Risk”, “High Risk”, Risk Assessments and DPIAs in the GDPR.....	17
4.1 The GDPR Definition of “Risk”	17
4.2 “High Risk” in the GDPR.....	19
4.3 Controller Accountability Obligations Calibrated by Risk	20
4.4 The Data Protection Officer and the Consideration of Risk	20
4.5 Specific GDPR Obligations Based on Risk	21
4.6 Specific Obligations for “High-Risk” Processing	22
4.7 Implicit GDPR Requirements for Risk Assessment	22
4.8 Guidance on Risk, High Risk and Risk Assessments.....	24
4.9 Obligations of EU DPAs to Promote Awareness of Risk	24
4.10 Risk Assessments as a Progressive Mechanism Under the GDPR.....	24
Part 2: The Risk-Based Approach of the GDPR in Practice	25
5. Identifying and Developing an Inventory of Risks and Harms	25
6. GDPR: Risk Level, “High Risk” and “Low Risk” Processing.....	28
6.1 Determining Risk Level Under the GDPR and Determining “High Risk”	28
6.2 “High-Risk” Processing List	30
6.3 “Low-Risk” Processing Lists	33
6.4 Requiring DPIAs for “High Risk” Processing Activities.....	33
6.5 Prior Consultation.....	35
7. Risk Assessments in Practice	36
7.1 Methodologies for Risk Assessments – General	36
7.2 Risk Assessment Methodologies in the Context of DPIAs.....	37
7.3 Other Considerations and Requirements for GDPR Risk Assessments	38
8. Risk Mitigation and Residual Risk.....	41
9. Demonstrating Compliance with the GDPR Risk Assessment Requirements	42
10. GDPR Risk Assessments and EU DPAs.....	42
11. Conclusion	43
Appendix 1.....	44

1. Introduction and Recommendations

The present guidance paper on risk, high risk and DPIAs has the following objectives:

- (1) to identify and analyse the GDPR provisions on risk, high risk, risk assessment and DPIAs;
- (2) to analyse the practical impacts, challenges and implementation in practice of these provisions; and
- (3) to provide suggestions on how these provisions can be consistently interpreted, implemented and enforced across Europe.

The paper is structured in two parts. Part 1 addresses the risk-based approach to data protection and privacy in general and identifies and explains the GDPR provisions on risk, high risk, risk assessments and DPIAs. Part 2 assesses the practical impacts and challenges associated with implementing these provisions in practice and makes suggestions on how these challenges can be resolved and where further guidance may be helpful.

At present, risk assessments are required under the EU Data Protection Directive. However, the GDPR broadens the relevance of risk, as it is explicitly based on the notion of a risk-based approach. Recital 74 of the GDPR states unambiguously that measures of controllers should take into account the risk to the rights and freedoms of natural persons. Various provisions in Chapter IV of the GDPR on the obligations of the controller and the processor specifically refer to “risk”, “high risk” and risk assessment (including data protection impact assessment). Thus, the GDPR effectively incorporates a risk-based approach to data protection, requiring organisations to assess the “likelihood and severity of risk” of their personal data processing operations to the fundamental rights and freedoms of individuals.

This does not mean that the protection of the rights of individuals (e.g. access, objection and erasure rights) depends on the risk level of the processing in question. Individuals’ rights apply in full irrespective of the level of risk in the processing. However, organisations will be required to modulate their data protection compliance according to the level of risk that their personal data processing operations pose to the fundamental rights and freedoms of individuals.

Indeed, many organisations already have been doing this as part of their internal compliance programs. The GDPR gives further impetus to this practice. Consequently, processing operations which raise lower risks to the fundamental rights and freedoms of individuals may generally result in fewer compliance obligations, whilst “high-risk” processing operations will raise additional compliance obligations, such as data protection impact assessments. In effect, this also links to the notion of “scalability” which envisages that the required compliance and accountability measures should take into account the nature, scope, context and purposes of the processing. Scalability and the risk-based approach are closely linked mechanisms incentivising accountability, based on the specificities of a particular processing operation.

By enabling prioritisation, risk assessments and the risk-based approach may also assist EU DPAs in discharging their regulatory and enforcement obligations more effectively. This will also create greater predictability and consistency in enforcement, which will, in turn, improve compliance practices and responses by businesses.

Finally, given the importance of the notion of risk in the GDPR and the need to implement these provisions consistently across the EU, the GDPR requires DPAs to create lists of the kinds of high-risk processing operations requiring a DPIA and allows them to issue such lists for low-risk processing. The GDPR also requires the European Data Protection Board (“EDPB”) to issue guidelines, recommendations and best practices on data breaches that may result in “high risk” to individuals.

The CIPL GDPR Project

This paper is produced by the Centre for Information Policy Leadership at Hunton & Williams LLP (“CIPL”) as part of its project (“CIPL GDPR Project”) on the consistent interpretation and implementation of the GDPR.

The CIPL GDPR Project—a multiyear-long project launched in March 2016—aims to establish a forum for dialogue amongst industry representatives, the EU DPAs, the European Data Protection Supervisor, the European Commission, the ministries of the member states and academics on the consistent interpretation and implementation of the GDPR through a series of workshops, webinars, white papers and reports.

As part of the CIPL GDPR Project work plan for 2016, CIPL aims to provide input to the Article 29 Working Party (“WP29”) on three of its priority areas: (a) DPO; (b) “high risk” and data protection impact assessments (“DPIAs”); and (c) certifications.¹

On 17 November 2016, CIPL issued a paper on the role of the DPO in the GDPR (“Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation”). On 30 November 2016, CIPL issued a paper on “The One-Stop-Shop and the Lead DPA as Co-operation Mechanisms in the GDPR”.

The present paper is the third within this series, giving input in a priority area of the WP29. This paper’s key suggestions and recommendations are designed to inform and support the WP29’s guidance on “high risk” and data protection impact assessments.

¹ See WP 29, “Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR)”, (Feb. 2, 2016) 442/16/EN, WP 236, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf.

Recommendations

1. GDPR Contexts Requiring Risk Assessment

- **Risk assessment is fundamental.** Under the GDPR, consideration of risk underlies organisational accountability and all data processing.
- **Specific obligations requiring risk assessment.** Organisations will have to conduct risk assessments as part of DPIAs for high-risk processing, as well as in connection with many other GDPR requirements, including data security, security breach notifications, privacy by design, legitimate interest, purpose limitation and fair processing.

2. Goal and Purpose of the “Risk-based” Approach

- **Prioritising compliance while maximising both privacy and effective use of data.** Risk assessment helps organisations to classify processing activities according to their risks to individuals, prioritise compliance and devise appropriate mitigations. As a core element of accountability, the risk-based approach enables organisations to maximise the potential benefits of processing and broader uses of data, while more effectively reducing any potential negative impacts on people.
- Any future regulatory guidance should seek to minimise unnecessary bureaucratic measures that would negate these benefits, while at the same time ensuring full protection of individuals’ fundamental rights.

3. General Points on DPA Guidance Regarding Risk Assessments and DPIAs

- **Balancing consistency and flexibility.** The guidance should create and facilitate as much consistency as possible, keeping in mind the context sensitivity of individual risk assessments and the resulting need for flexibility.
- **Industry input.** To ensure effective implementation, specific risk guidance should be developed in collaboration with responsible organisations that are experienced in risk management and committed to organisational accountability and data protection.
- **Avoiding prescription.** Guidance on DPIAs should provide for flexibility, especially since risks may vary over time, across industries and regarding purposes, and avoid overly complex specifications. Overly complex guidance may encourage some organisations to interpret “high risk” too narrowly to avoid burdensome DPIAs, which would undermine the objective of encouraging organisations to systematically assess risk to data subjects.
- **Technology neutral and future proof.** The risk-based approach embedded in the GDPR ensures that the GDPR remains technology neutral and future proof so that the rules can be applied flexibly to different technologies and business practices based on risk. All measures designed to implement GDPR risk assessment requirements should aim to preserve this feature.

4. Identifying the Risks and Harms

- **Common risk and harm identification.** The GDPR provides guidance on “risky processing activities” that may result in harm, as well as on the nature of these harms. In addition, CIPL and other organisations have developed classifications of risks, threats and harms to consider in a risk assessment (see example on p. 15). A common risk identification and classification system (with respect to the risky processing activities, threats and harms) should be developed, enabling organisations to define the scope of risk management within their organisations and to have a repeatable and consistent framework to identify risks to individuals (and the organisation) in multiple scenarios and over time.
- **Collaborative development of a risk and harm classification.** Risk identification and classification for purposes of GDPR compliance would benefit from further collaborative development and guidance by all stakeholders, including industry and the DPAs. Achieving a high degree of consistency and agreement in the identification and classification of the relevant risk elements—the “risky processing activities” and threats, as well as the types of harms that might result—is both desirable and possible. This is because such identification and classification will mostly occur within the context of similar practices and shared legal norms and cultural values across the EU.
- **Industry-specific risk identification.** A voluntary, collaborative and agreed identification of risk elements might also be possible within certain industry sectors, based on common processing activities within a sector.
- **Preserving context-specific flexibility.** Even with a widely agreed identification and classification of risks, threats and harms, each organisation must have the flexibility and obligation to consider any additional risk elements that are specific to its own business, scope, context and processing.
- **Considering the global context.** For many global organisations, the risks and harms they consider might also be impacted by their operations in other regions and the need to respect different legal regimes and cultural expectations. As organisations roll out new products and services globally without variation between countries, their risk assessments must be able to assess comprehensively the global impact of a product or a service. Any further DPA guidance on the elements and methodology of risk assessment must be workable in that context without adversely impacting the level of protection of the individuals in the EU.

5. Types of Harms – Material, Non-Material and Societal

- **Material and non-material harms.** The identification and classification of harms should include both material and non-material (tangible and intangible) harms. Material harms may require prioritisation over non-material harms, depending on context.
- **Societal harms.** The consideration of societal harms (e.g. loss of social trust) is not a GDPR requirement and organisations should not be expected to consider societal harms in their risk assessments. However, the consideration of societal harms may be relevant and could be considered in appropriate circumstances. In such cases, difficult issues concerning the definition, identification and concreteness of such harms and whether organisations are well placed to assess them, must be resolved by organisations, for example, by identifying criteria and proxies for such societal harms that are objective and measurable. In addition, it must be clear that any

consideration of societal impacts and harms must remain grounded in concrete risk to individuals, which, in turn, may have wider societal implications.

6. Establishing a Risk Assessment Methodology and Process

- **A flexible methodology.** The actual process or methodology of risk assessment, i.e. how the various risky activities or threats and harms should be assessed, weighed and evaluated, should largely be left to individual organisations. Any guidance on the risk assessment process or methodology must be principles based, high level and flexible, leaving it to individual organisations or industry sectors to develop or adopt specific processes that work in their contexts and that can be integrated into their broader organisational risk management programs.
- **Considering existing guidance.** It may be beneficial to consider existing regulatory guidance from EU DPAs on risk assessment methodology, including on the privacy impact assessments, or from other regulated areas, such as environmental or financial, to the extent they are relevant and helpful in providing frameworks for assessment.
- **Sector-specific methodologies.** Particular sectors (e.g. health, banking, etc.) could use such principles-based methodologies to develop sector-specific guidance if needed to reflect the specificities of their sectors. However, such sector-specific guidance should also not be too prescriptive and should give organisations the necessary latitude to adapt the methodology for their own contexts.
- **User-friendly methodologies.** Risk assessment methodologies must be easy to understand and to use by experts and non-experts from various parts of an organisation, including compliance, IT, marketing, HR, data scientists, privacy engineers, etc. The methodologies should not necessarily be resource intensive to ensure they can be easily embedded in the relevant organisational processes.

7. Accounting for Proportionality Between Risks and Benefits

Proportionality between risks and benefits. While the GDPR does not provide guidance on how to evaluate and assign weight to the various risks and harms in the context of the DPIA requirements, it does provide that any evaluation must take into account the proportionality between risk/harm and the purposes, interests or benefits that are being pursued. This is also consistent with the WP29 Opinion on “legitimate interest”. Thus, the same risk may be scored differently when compared to a low benefit or a high benefit.

- **Considering benefits at the outset.** All risk assessments must include a consideration of the benefits of processing, including the benefits to individuals, the organisation, third parties and society, to enable the preservation of the desired benefits when implementing any necessary mitigations to address the identified risks. Benefits should be considered at the outset of the risk assessment as they are related to the purpose of the processing. The benefits and purposes of the processing must be kept in mind when devising mitigations to avoid unnecessary reduction of the benefits or undermining of the purposes.

8. Considering Reticence Risk

- **Reticence risk.** Any further guidance should recognise the importance of considering reticence risk or the risk of not engaging in processing. However, accountable organisations must be able to demonstrate how and why they reached their conclusions regarding reticence risk.

9. Responsibility for, and Decisions Based on, Risk Assessments in the Organisation

- **Responsibility for risk assessments in an organisation.** The DPO² has an obligation to advise in respect of DPIAs, but is not required to carry out DPIAs by himself or herself or be exclusively responsible for them. It is likely that others in the organisation will carry out preliminary risk assessments and then escalate complex or high-risk matters to the DPO. Risk assessment tasks should be delegated across the organisation, as appropriate. The role of the DPO should be to define high-level guidelines or methodology and to ensure monitoring and evidencing of the DPIAs and their outcome, including residual risk.
- **Decisions based on risk assessment.** Decisions based on risk assessments about risk mitigations and whether to proceed in light of any residual risk will likely have to involve an organisation's management in consultation with the DPO. In the case of disagreement, the issue will have to be raised with the "highest level of management" under the GDPR.

10. Documenting Risk Assessments

- **Evidencing and demonstrating risk assessments.** Risk assessments, including the DPIAs, must be documented in every case and every situation where they are required explicitly (e.g. DPIA, breach notification, privacy by design) and implicitly (e.g. legitimate interest processing and fair processing) under the GDPR. On request, organisations must be able to demonstrate, both internally and externally, to EU DPAs and individuals, how they have carried out these risk assessments.

11. Determining "High Risk"

- **Default criteria for "high risk".** Future guidance should clarify that organisations can "rebut" the presumption of high-risk processing in Article 35(3)(a) through an initial risk assessment taking into account nature, scope, context and purpose of the specific processing at issue. The actual risk level (i.e. the "likelihood" and "severity" of any harm) and whether a given processing is, in fact, "high risk" must be determined in light of the specific circumstances at hand by taking into account: (a) the nature, scope, context and purposes of the processing and (b) the ability to mitigate a "high risk", for example in contexts where the absence of such ability would trigger the "prior consultation" requirement under the GDPR. The organisation's judgement of whether the specific circumstances give rise to high-risk processing should be taken into account.
- **Interpreting the GDPR's "high risk" examples.** Future guidance should clarify that the GDPR's terms of "large-scale" processing, "systematic and extensive evaluation" and "systematic monitoring" require organisations to interpret them on a case-by-case basis and in the context of

² References in this paper to the "DPO" or to various DPO tasks and obligations may also apply to chief privacy officers and other relevant privacy professionals in an organisation who are not formal "DPOs" under the GDPR and have privacy accountabilities and responsibilities assigned by the organisation.

their own operations, recognising that organisations must be able to justify their interpretations. The Article 29 Working Party identified—in connection with the designation of a mandatory DPO—a set of factors to consider in determining whether processing operations are “large scale” and entail regular and systematic processing.³ The guidance in relation to high risk, specifying the “systematic-extensive-large-scale” criteria, should be consistent with the DPO criteria.⁴ In effect, the terms largely overlap with the criteria for designating a mandatory DPO.⁵

- **High risk and new technologies.** Further guidance on high risk should clarify that “using new technology” cannot be the sole trigger for high-risk status requiring a DPIA, but must be coupled with additional high-risk characteristics.
- **Avoiding duplicative risk assessment for similar processing.** Any guidance on DPIAs should clarify that organisations are allowed to carry out a single DPIA for a set of similar processing operations with similar risk levels, as long as they are able to demonstrate the rationale for their interpretation and action.

12. Lists of High-Risk and Low-Risk Processing

- **Nature of high-risk processing lists.** Any future EU DPA “lists of the kind of processing operations” that are subject to the DPIA requirements (i.e. “high risk”) should recognise that risk is context specific. Thus, such future lists should not enumerate specific per se high-risk activities, but should, instead, set forth either (a) criteria for high-risk processing that must be evaluated in each case through risk assessments or (b) presumptive high-risk activities that the controller can rebut through a risk assessment. (See Figure 1, Section 6.2.8 and Table 4, Section 6.2.9)
- **Lists of low-risk processing.** It may be helpful for EU DPAs to establish criteria, examples or lists of processing where a DPIA is not required (because there is “low risk”). To the extent DPAs have already characterised certain processing activities as common, frequent or low risk, such as HR data or customer relations data, any future guidance on low risk should be consistent with such earlier guidance.
- **Avoidance of negative inferences.** Any lists should explicitly state that absence from the particular list does not mean that a criterion or type of processing falls into the opposite category, i.e. absence from a “high risk” list does not automatically mean “low risk”, and absence from a “low risk” list does not automatically mean “high risk”.

13. DPIAs for High-Risk Processing Activities

- **Stages of DPIA risk assessment.** Both current practice and, possibly, the GDPR, suggest a two-staged process in connection with a DPIA. First, there is a screening process or initial risk

³ Article 29 Working Party, Guidelines on Data Protection Officers (“DPOs”), 13 December 2016, WP 243, at 2.1.3 and 2.1.4.

⁴ Our views are without prejudice to possible further CIPL comments or further possible changes on the guidance on the mandatory DPOs.

⁵ See CIPL paper of 17 November 2016, Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf.

assessment to determine whether there is high risk requiring a DPIA. Second, if the screening process indicates that a DPIA is needed, then the next step is a full-blown DPIA, which also includes a risk assessment, as well as applying mitigations. (See Diagram 1, Section 6.4.2)

- **Timing of consideration of mitigations.** A point of clarification in any guidance may be how to distinguish between the initial risk assessment or screening process to determine the need for a DPIA and the risk assessment as a component of the DPIA itself, particularly with respect to mitigations and residual risk. If an organisation manages to mitigate risk in the stage of the initial risk assessment or screening and to eliminate “high risk” in that stage, then no DPIA would be necessary. In other words, if the initial assessment thoroughly considers these risks, then fewer activities will need a full DPIA, and vice versa.

14. Prior Consultation

- **Limiting prior consultations.** The requirement to consult with the DPA if a high-risk processing cannot be mitigated amounts to a prior authorisation requirement. To avoid overburdening both the organisations and the DPAs, prior consultations should be the exception and not the rule.
- **Informal consultations.** It would be helpful for the WP29 to maintain the ability for organisations to seek informal consultations and dialogue with DPAs, in addition to formal consultations. Such informal consultations are consistent with the tasks of the DPO to co-operate or consult with the DPA and are essential for the concept of one-stop-shop and lead authority.

15. Seeking the Views of Individuals or Their Representatives in DPIAs

- **Flexibility in seeking views of individuals.** Article 35(9) provides that, “where appropriate”, organisations should seek “the views of individuals or their representatives”. This may be problematic for private sector organisations (including and especially ones that do not have direct relationships with individuals), and more suited for public sector bodies. Organisations should be allowed flexibility in how they implement this requirement based on factors such as business models, trade secrets and IP rights. In some cases, there may be an opportunity for soliciting such views as part of trial roll-outs prior to formal roll-out.

16. Mitigating Risks

- **Selecting the mitigations.** Organisations must consider a wide range of risk mitigation measures, ranging from pseudonymisation, data minimisation and security measures, to various data governance or oversight mechanisms. The appropriate mitigation measures depend on context and should be chosen on a contextual basis, taking into account the risks involved, the cost of implementing and the effectiveness of these measures, their impact on the purposes, interests or benefits that are being pursued, and also the reasonable expectations of individuals, transparency, and the elements of fair processing.
- **Risk mitigation, not elimination.** Risk mitigation does not mean the elimination of risk but the reduction of risk to the greatest reasonable extent, given the desired benefits and reasonable economic and technological parameters. Organisations will have to make a reasoned and evidenced decision whether to proceed with processing in light of any residual risks, taking into account “proportionality” vis-à-vis purposes, interest and/or benefits.

17. Consent and Risk

- **Effect of valid consent.** If an individual has given valid consent to a processing activity, it can be used as indication that he or she has agreed to the corresponding risk in appropriate contexts.

18. Risk Assessments and the DPAs

- **Multiple risk applications for DPA.** EU DPAs should be able to understand and conduct risk assessments and employ a risk-based approach in the performance of their statutory obligations with respect to: (a) evaluating the risk assessments of organisations; (b) assessing fines in proportion to risk level; and (c) prioritising their own oversight and enforcement activities in a way that is transparent to regulated organisations.

PART 1

THE RISK-BASED APPROACH TO DATA PROTECTION AND PRIVACY

2. An Overview of the Risk-Based Approach to Data Protection and Privacy

Since the 1980s, risk management has played an increasingly important role in ensuring the compliance of organisations with data protection laws and protection of the fundamental rights and freedoms of individuals. Risk management refers to the process of systematically identifying, managing and mitigating the impact of a personal data processing operation on the organisation, and increasingly on individuals. Organisations have been managing the risks of data protection and non-compliance to their own organisations and operations through well-formulated and documented enterprise risk management (ERM) processes. Increasingly, organisations have also started to include in these processes the assessment of the risks and harms to individuals, as an important and a novel aspect of proactive privacy and data protection risk management.⁶

In recent years, with the proliferation of information communication technologies and the complex data protection problems they raise, risk management has taken an even more prominent role in various data protection law regimes. Correspondingly, a sizeable body of requirements and guidance on the subject of privacy risk management has already been developed in various contexts.⁷ The risk-based approach, which was foreshadowed in elements of the EU Data Protection Directive and is now fully enacted by the GDPR, confirms this trend. Therefore, when determining how to implement the risk-based approach of the GDPR and how to identify, manage and mitigate risks, it is important to build upon and take into account current laws, research and guidance on risk, risk assessment and data protection impact assessments (“DPIAs”) in the field of data protection.

2.1 Advantages of a Risk-Based Approach to Data Protection

A risk-based approach to data protection and privacy has numerous advantages:

- a. The risk-based approach is first and foremost an effective tool for ensuring a high level of protection of the rights and freedoms of individuals. It enables all stakeholders to dedicate their resources to the areas where the risks and potential harms for individuals are most significant and to mitigate these risks. This in turn creates better outcomes and more effective protection for individuals.

⁶ Over the past three years, the Centre for Information Policy Leadership at Hunton & Williams LLP (CIPL) has hosted a series of multinational workshops and published three white papers on risk management and its role in effective modern data protection. CIPL, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice* (2014), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf; see also CIPL, *The Role of Risk Management in Data Protection* (2014), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf; CIPL, “Protecting Privacy in a World of Big Data – the Role of Risk Management”, discussion draft, February 16, 2016, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_2_the_role_of_risk_management_16_february_2016.pdf.

⁷ Examples of privacy risk management sources are included in Appendix I. (Examples of existing Sources on Risk Management).

- b. By assessing the likelihood and significance of the impacts (both positive and negative) and any potential harms to individuals of a specific personal data processing activity, risk assessment helps organisations to devise effective and appropriate mitigations and controls. This approach ensures that organisations can maximise the potential benefits of the processing activity whilst reducing the potential negative impact of the activity in question on the rights and freedoms of individuals.
- c. A risk-based approach to data protection enables a flexible and context-specific approach towards compliance. It enables organisations to prioritise tasks and allocate their resources effectively whilst protecting the fundamental rights and freedoms of individuals.
- d. Adopting a risk-based approach to data protection promotes innovation. It enables organisations to adopt required protective measures that minimise the risk level to individuals of their personal processing operations only to the extent necessary.
- e. A risk-based approach is also relevant for data protection authorities. Where appropriate, European data protection authorities (“EU DPAs”) can use risk management to prioritise the fulfilment of their advisory and supervisory tasks. The risk-based approach makes it possible for DPAs to deploy their resources in the most effective and consistent manner and in the areas where there is a higher likelihood and severity of risks and harms to individuals. Of course, there may be situations in which some EU DPAs may be obliged to act independently of risk, such as, possibly, in a response to a complaint from individuals.
- f. A risk-based approach to data protection enables organisations to translate abstract concepts and goals into concrete risks and implementable mitigating controls and steps that can easily be understood by non-privacy experts (including business and product development, data scientists, IT teams) in an organisation. It enables organisations to embed data privacy across all their operations in an understandable manner, thereby delivering more effective and relevant protections for individuals.

3. What is “Risk”?

3.1 Defining Risk

- 3.1.1 There is no agreed definition of the notion of “risk” in the data privacy field. As stated, the GDPR also does not define the concept of “risk” and, instead, offers interpretative guidance on what may constitute risk and harms to individuals.
- 3.1.2 The concept of “risk” appears to mean different things to different people, especially in a subjective domain like privacy, and is often used flexibly to apply to different components of “risk”. For example, one might refer to the risk of a data breach, but the data breach itself does not necessarily lead to harm or damage for data subjects, depending on whether the data are ever looked at, used or encrypted. On the other hand, one might refer to the risk of a loss of confidentiality or of financial loss, which are harms or damages that could result from a data breach.
- 3.1.3 Similarly, “risk” is sometimes broadly used to refer to a risky processing activity or a “threat” that could result in a harm for the individual, or to the harm itself, or to both. That is also the

approach that appears to be taken in Recital 75 of the GDPR, which seems to conflate the concepts of risky processing activity and harm under the rubric of “risk”.⁸

- 3.1.4 Relatedly, a definition of risk that has been used in the privacy community and proposed both for purposes of this paper and application of the GDPR is as follows: privacy risk equals the probability that a data processing activity will result in an impact, threat to or loss of (in varying degrees of severity) a valued outcome (e.g. rights and freedoms). An unacceptable privacy risk, therefore, would be a threat to, or loss of, a valued outcome that cannot be mitigated through the implementation of effective controls and/or that is unreasonable in relation to the intended benefits.
- 3.1.5 The concept of “unacceptable risk” is relevant because the purpose of all risk assessments necessarily cannot be to eliminate all risk but to identify and eliminate unacceptable risk. Expressed differently, the purpose of risk assessment is to reduce risk as much as reasonable and practicable in light of the intended benefits and the available mitigations and controls, including state-of-the-art technology, cost of implementation and best practices.
- 3.1.6 While there are numerous definitions and concepts of “risk” in the privacy and data security arena, the GDPR clearly focusses on one type of risk: adverse risk to the individual. Accordingly, we will focus in this paper on this aspect, noting that the assessment of the risks to individuals is closely related to other aspects of risk, especially as organisations incorporate their GDPR-based risk assessments that focus on adverse risks to individuals into their broader enterprise risk management systems that assess mainly risks to the organisation (such as reputational, financial and litigation risk) or corporate opportunity risks related to the organisation’s business and profit objectives. Note also, for example, that existing practices and guidance on data protection impact assessments (DPIA) make clear that risk assessments under a DPIA may go beyond assessing the risks to individuals, but may assess the risks of a wider set of stakeholders, including the risk to the organisation itself or to society at large.⁹

3.2 **Identifying the Elements of Risk (risky processing activities, threats and possible harms)**

3.2.1 Risks and Harms¹⁰

A key challenge of privacy risk assessments is deciding what risks and harms to individuals to consider, how to weigh them and how to assess the likelihood and severity of the harm. While the GDPR provides, in particular in its Recital 75, guidance on what is considered risky or high-risk processing, this guidance logically is quite general. It does not address how to go about identifying and weighing particular risks and harms that are associated with data

⁸ The Oxford English Dictionary defines risk as “a chance or possibility of danger, loss, injury or other adverse consequences.” Oxford English Dictionary, Online Version. This definition arguably reflects a broad concept of risk, encompassing both the underlying actions (or risky processing activities or threats) that may result in harm, as well as the actual harm itself. However, this definition is also limited because it omits the flip side of risk: a larger benefit, reward or payoff. Thus, it is important to keep in mind that accepting risks can also result in positive outcomes.

⁹ See, e.g. UK ICO, “Conducting privacy impact assessments code of practice”(February 2014), pp. 7, 23-26.

¹⁰ We use the term “harms” in this paper in a generic sense, encompassing all potential adverse effects, including material and non-material (or tangible and intangible) effects and impacts of data processing.

processing. Thus, part of the challenge in implementing the risk provisions of the GDPR will be to achieve consensus on the specific risks and harms to individuals that risk management is intended to identify and mitigate. This is a critical first step for every organisation, including for EU DPAs who will have to oversee and enforce the implementation of these rules consistently across Europe.

3.2.2 It is possible and helpful to identify and enumerate general and broadly relevant risk categories. Such identification and enumeration enable both organisations and DPAs to identify and evaluate the specific risks associated with a specific processing activity throughout the entire data cycle (from collection, storage, use and sharing, to disposal) in a repeatable and consistent manner. It also helps organisations to define the scope of their risk management operations.

3.2.3 In the Centre for Information Policy Leadership’s 2014 white paper *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*, we offered a preliminary matrix of tangible and intangible harms that might be considered.¹¹ This example of a “risk matrix” was meant to illustrate a framework for identifying in the horizontal column the various threats and in the vertical column the potential harms that could result and to assess their respective likelihood and severity. We believe that this initial matrix is consistent with the relevant GDPR guidance on what constitutes risk set forth in Sections 4.1 and 4.2.

3.2.4 CIPL Risk Matrix

Version 1.0 06/2014		DRAFT - Risk Matrix									
		Unjustifiable Collection			Inappropriate Use			Security Breach			Aggregate
					Inaccuracies Not expected by individual Viewed as Unreasonable Viewed as Unjustified			Lost Data Stolen Data Access Violation			
Threats											
Harms		Likely	Serious	Score	Likely	Serious	Score	Likely	Serious	Score	Risk Rank
Tangible Harm											
Bodily Harm		0	0	0	0	0	0	0	0	0	0
Loss of liberty or freedom		0	0	0	0	0	0	0	0	0	0
Financial loss		0	0	0	0	0	0	0	0	0	0
Other tangible loss		0	0	0	0	0	0	0	0	0	0
Intangible Distress											
Excessive surveillance		0	0	0	0	0	0	0	0	0	0
Suppress free speech		0	0	0	0	0	0	0	0	0	0
Suppress associations		0	0	0	0	0	0	0	0	0	0
Embarrassment/anxiety		0	0	0	0	0	0	0	0	0	0
Discrimination		0	0	0	0	0	0	0	0	0	0
Excessive state power		0	0	0	0	0	0	0	0	0	0
Loss of social trust		0	0	0	0	0	0	0	0	0	0

Legend:
 Rank 'Likely' from 10 (high) to 1 (low) based on the highest score for any component
 Rank 'Serious' from 10 (high) to 1 (low) based on the highest score for any component

Aggregate Risk Rank:
 Highest score is 300
 Lowest score is 0

Table 3: CIPL Risk Matrix

¹¹ CIPL, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice* (2014), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf.

Numerous other similar efforts to identify relevant risks, impacts and harms have been made in recent years.¹² However, there remains an ongoing need for additional thinking on what constitutes a risk, harm or impact that a risk management framework should seek to minimise or prevent when evaluating data processing.

There are a wide range of possibilities for what might constitute a **harm**, but it seems clear that the term includes:

- a) **tangible, physical and material harms** (including financial or economic loss, physical threat or injury, unlawful discrimination, identity theft, loss of confidentiality and other significant economic or social disadvantage); and
- b) **intangible and non-material harms** (such as damage to reputation or goodwill, or excessive intrusion into private life).

There are some suggestions that broader **societal harms** could also potentially be included. Defining societal harms is difficult. They could include the contravention of national and multinational human rights instruments, loss of social trust, damage to democratic institutions or any aggregate impact of harms to individuals. Including societal harms in risk assessment is controversial, primarily for practical reasons having to do with defining societal harms generally and requiring private sector organisations to identify and evaluate such harms specifically. In any event, there must be a link to the individuals' privacy, as will be further explained in Section 5.

Going forward, it is important that the meaning of risk and harm be defined through transparent, inclusive processes and with sufficient clarity to help guide organisations in their risk analyses and mitigation, including in the context of implementing the GDPR.

3.2.5 Benefits

In addition to assessing potential risk and harms, it is important for both organisations and DPAs to examine the benefits (or purposes) of data processing activities systematically and objectively. For organisations, this should typically occur at the outset of any risk management process, because without understanding the benefits and purposes of a processing at stake, it is impossible to determine the appropriate level of mitigations or controls for the risks of harms to individuals. Further, after mitigating such risks to the appropriate level in light of the identified benefits, it must be determined if any residual risks of harm are acceptable.

As with harms, this assessment of benefits should include both the magnitude of benefit and its likelihood of occurring. The range of benefits should include:

- a) **benefits to individuals** (e.g. ability to complete a transaction, obtain a desired good or service, be protected from fraud, enjoy greater efficiency or convenience, and access improved medical treatment and prevention);

¹² See e.g. National Institute of Standards and Technology (NIST) Internal Report 8062 (DRAFT), *Privacy Risk Management for Federal Information Systems*, May 2015, http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf.

- b) **benefits to the organisation** (e.g. ability to attract customers, deliver goods or services more efficiently, ensure compliance with other laws and reduce fraud and other legal and commercial risks); and
- c) **benefits to society more broadly** (e.g. use of data for social good and development, such as reducing the spread of infectious diseases; enhancing research in health care and other areas that benefit the public; guarding against terrorism, fraud, cyber crimes and other crimes; reducing environmental waste; delivering services to the public with greater efficiency and fairness; etc.).

3.2.6 Competing Rights

Relatedly, the risk analysis might also include consideration of other (fundamental) rights that have to be ensured, including in situations where such rights may be in competition with privacy or data protection rights and interests. For example, intellectual property rights, or the right of freedom of expression or information, may have to be balanced against the right to privacy when considering whether to use personal data for certain purposes or make them publicly available.

4. “Risk”, “High Risk”, Risk Assessments and DPIAs in the GDPR

In this section, we identify and analyse the relevant provisions on “risk”, “high risk”, risk assessments and DPIAs in the GDPR.

4.1 The GDPR Definition of “Risk”

The GDPR does not define the notion of “risk”, but the recitals and the substantive provisions include indications of the types of risks and harms to individuals to be considered.

Table 1 below lists the **GDPR provisions on risk**:

Aspect	Particulars
Risk Definition (Recital 75)	The risks to the rights and freedoms of individuals of “varying likelihood and severity” may result from personal data processing which could lead to “physical, material or non-material damage” (Recital 75)
Non-exhaustive list of examples of such “physical, material or non-material damage” and of processing activities that could result in such damage (Recital 75)	<ul style="list-style-type: none"> • Discrimination • Identity theft / fraud, financial loss • Reputation damage • Loss of confidentiality of personal data protected by professional secrecy • Unauthorised reversal of

	<p>pseudonymisation</p> <ul style="list-style-type: none"> • Any other significant economic or social disadvantage • Individuals deprived of rights and freedoms, or prevented from exercising control over their data • Processing sensitive data, including data on racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership; genetic data; health data; data concerning sex life; or data on criminal convictions and offences or related security measures • Profiling (personal aspects are evaluated [e.g. analyse or predict work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements] to create or use personal profiles) • Processing children’s and vulnerable persons’ data • Processing large amounts of data affecting large numbers of individuals
Additional examples of risks (Article 32.2)	<ul style="list-style-type: none"> • Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data
Factors to take into account when determining risk level (i.e. likelihood and severity of risk) (Recital 76)	<ul style="list-style-type: none"> • Nature; • Scope; • Context; and • Purposes of processing.
Risk or High Risk (Recital 76)	<ul style="list-style-type: none"> • Objective assessment

Table 1: Risk in GDPR

4.2 “High Risk” in the GDPR

There is no definition of “high risk” in the GDPR. However, some indication of the meaning of risk can be found in several GDPR recitals and articles.

Table 2 sets out the **GDPR provisions on “high risk”**:

Aspect	Particulars
What types of processing <i>may</i> result in “high risk”?	<ul style="list-style-type: none"> • Each of the risks in table above can become “high risk”, depending on the “likelihood and severity” of the risks as determined in a risk assessment process by reference to the nature, scope, context and purpose of processing; • Processing, “particularly using new technologies”,¹³ might result in “high risk”, depending on “nature, scope, context and purposes of the processing” (“high risk” processing requires an “assessment of the impact” [a DPIA] of the proposed processing operation);¹⁴ • New “kind” of personal data processing operation where no DPIA has been conducted or where a DPIA has become necessary over time on the basis of the time elapsed since initial processing;¹⁵ and • Large-scale processing operations at regional, national or supranational level and which could affect a large number of data subjects.¹⁶
Examples of “high risk processing” [Article 35(3)]	<ul style="list-style-type: none"> • “[S]ystematic and extensive evaluation of personal aspects ... based on automated processing, including profiling, on which decisions are based

¹³ When “new technologies” are privacy enhancing technologies, they may not qualify as a basis for finding “high risk.”

¹⁴ Article 35(1) GDPR

¹⁵ Recital 89, GDPR

¹⁶ Recital 91, GDPR

	<p>that produce legal effects ...”;</p> <ul style="list-style-type: none"> • Large-scale processing of sensitive personal data as well as criminal conviction and criminal offence data; and • Large-scale and systematic monitoring of a publicly accessible area.
--	---

Table 2: “High Risk” in GDPR

4.3 **Controller Accountability Obligations Calibrated by Risk**

4.3.1 Article 24(1) requires controllers to implement “appropriate technical and organisational measures” to ensure and demonstrate compliance with the GDPR by taking into account the “nature, scope, context and purposes of processing” and the “risks of varying likelihood and severity for the rights and freedoms” of individuals.

The controller also has the obligation to review and update these measures “where necessary”.

4.3.2 This general accountability provision implies, according to CIPL’s earlier work on accountability, that a controller must build, implement and be able to demonstrate a comprehensive data privacy program (e.g. leadership and oversight, policies and procedures, training and awareness, monitoring and verification, response and enforcement) based on several factors, including specifically the risk level to the fundamental rights and freedoms of individuals.¹⁷

4.3.3 This will allow organisations to calibrate or modulate their compliance program based on risks, harms and benefits to individuals and to focus their attention and resources even further on processing that creates risks and high risks to individuals. This does not absolve the organisation from the overall obligation to comply with the GDPR in respect of processing. It only means that the actual controls, compliance steps and verifications will be more intensive in respect of processing that creates risks or high risks to the fundamental rights of individuals. This also means that the actual privacy compliance programs may vary between different organisations based on the various levels of risk associated with their processing.

4.4 **The Data Protection Officer and the Consideration of Risk**

Under Article 39(2), the data protection officer (“DPO”) has a duty to take into account the risks to the fundamental rights and freedoms of individuals when performing his or her GDPR tasks. This means that DPOs must consider risk when performing their advisory, training and monitoring tasks as well as their obligations to co-operate with EU DPAs. DPOs will need to prioritise tasks which involve

¹⁷ CIPL, The Role of Enhanced Accountability in Creating a Sustainable Data-Driven Economy and Information Society (2015); https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_1_the_role_of_enhanced_accountability_21_october_2015.pdf

personal data processing operations that create more risks to the fundamental rights and freedoms of individuals.

4.5 **Specific GDPR Obligations Based on Risk**

The GDPR imposes a number of obligations on both controllers and processors which require them to assess the risks posed by their personal data processing operations to the rights and freedoms of individuals.

4.5.1 Data Protection by Design

To decide how to implement data protection by design, Article 25(1) requires the controller to take into account various factors including the risks of their personal data processing operation to the fundamental rights and freedoms of the individuals.

4.5.2 Data Security

Article 32(1) on the “security of processing” provides that controllers and processors must consider, among other factors, the risks to the fundamental rights and freedoms of individuals that are associated with their processing activities and must implement “appropriate technical and organisational measures to ensure a level of security appropriate to the risk”. (Other listed factors to consider are: “state of the art, the cost of implementation and the nature, scope, context and purposes of processing”.) This provision is in line with and elaborates Article 17 of the current Data Protection Directive.

Article 32(2) provides that controllers and processors have to take into account the risks of their personal data processing operations when determining the appropriate level of security, in particular, the risks that may arise from “accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed”.

Processors are furthermore required to assess the risks of processing as a matter of a contractual obligation in contracts with controllers. Specifically, Article 28(3)(c) provides that processors must be required by contract to implement the security measures provided by Article 32 by considering several factors, including the risk that the personal data processing operation poses to the fundamental rights and freedoms of individuals.

Article 28(4) sets forth the same requirement for sub-processors.

4.5.3 Data Breach Notification to European Data Protection Authorities (“EU DPA”)

Article 33 provides that the controller must notify the EU DPA of the data breach without undue delay or not later than 72 hours after becoming aware of it, if a breach results in a risk to the rights or freedoms of individuals.

4.5.4 Appointment of Representative of Controller or Processor Established Outside the EU

Article 27(2)(a) provides that where processing, in addition to other factors, is “unlikely to result in a risk to the rights and freedoms” of individuals, “taking into account the nature, context, scope and

purposes of the processing”, a controller or processor not established in the EU does not have to designate a representative in the EU.

However, this exception to the requirement to designate an EU representative does not apply to large-scale processing of sensitive personal data or data relating to criminal convictions or offences, nor to processing of public authorities or bodies.

4.6 **Specific Obligations for High-Risk Processing**

The GDPR has specific obligations which are triggered only in cases of high-risk processing.

4.6.1 Security Breach Notification to Individuals

Under Article 34(1), controllers have an obligation to notify individuals of a data breach in cases where such a breach “is likely to result in a high risk to the rights and freedoms” of the individuals.

4.6.2 DPIA

Article 35(1) provides that controllers have the obligation to conduct DPIAs for processing which is likely to result in high risk to the rights and freedoms of individuals taking into account the nature, scope, context and purposes of the processing. Data processing that may be “high risk” was set forth above in Table 2 and includes use of new technologies, new types of processing, large-scale processing, automated processing and profiling, processing of sensitive data and large-scale and systematic monitoring of public areas.

4.6.3 Prior Consultation With EU DPAs for “High Risk” Processing That Cannot Be Mitigated

Where a DPIA indicates that the processing would result in “high risk” and the controller cannot mitigate the risk, the controller must consult with the EU DPAs.¹⁸ It is the controller’s responsibility to determine whether the risk cannot be mitigated.¹⁹

4.7 **Implicit GDPR Requirements for Risk Assessment**

Under the GDPR, controllers will have to conduct a risk assessment in various cases by virtue of the specific requirements, although risk assessment is not explicitly mentioned in these provisions.

4.7.1 Legitimate Interest Balancing Test

Processing can be lawful under Article 6(1)(f) on the ground of “legitimate interest” if the processing 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. In order for controllers to determine whether they can rely on this ground for processing, they need to conduct a balancing test to assess whether their legitimate interests are overridden by the interests or fundamental rights and freedoms of the data subject. The balancing test will require the controller to understand if the interests of organisations outweigh the

¹⁸ Article 36(1).

¹⁹ Recital 94

fundamental rights and freedoms of individuals. This balancing test will have to include the consideration of risks and harms, or adverse impacts on individuals and cannot be performed without conducting a risk assessment.

4.7.2 Purpose Limitation – Determining Compatibility of Subsequent Purposes

Article 6(4)(d) provides that in considering the compatibility of a new purpose, the controller must take into account, among other factors, “the possible consequences of the intended further processing for data subjects”. These consequences include any risks, harms and adverse impacts on individuals implicitly. Hence, organisations will have to conduct a risk assessment in order to help determine the compatibility of the subsequent processing.

4.7.3 Fair Processing Requirement

In order to determine if a processing is fair, as required by the first data protection principle in Article 5, controllers may have to assess among other things the impact and consequences for individuals, including any risks and harms to them. Hence, a risk assessment may become an integral part of the fair processing assessment.²⁰

4.8 Guidance on Risk, High Risk and Risk Assessments

The GDPR provides the following instances where there will be future development of rules and interpretative guidance on risk from a number of stakeholders:

- a) Article 35(4) provides that the European DPAs “shall establish and make public a list of the kind of processing operations that are subject to” DPIA requirements, i.e. that are “high risk”. Additionally, under Article 35(5), EU DPAs may also provide a list of processing for which DPIAs are not required.
- b) Article 40(2)(h) provides that codes of conduct may address risk assessments.
- c) Article 70.1(h) provides for the EDPB to issue guidance on the circumstances in which a personal data breach is likely to result in high risk.
- d) Finally, controllers have to seek the advice of their DPO when undertaking a DPIA. This means that DPO will also provide internal guidance on risk levels and risk assessments.

4.9 Obligations of EU DPAs to Promote Awareness of Risk

Article 57(1) provides that EU DPAs have the obligation to promote public awareness and understanding of various matters, including risks related to personal data processing. Such informational activities shall in particular address the specific case of children.

4.10 Risk Assessments as a Progressive Mechanism Under the GDPR

Because the application and outcomes of risk assessments are context specific, such risk assessments help ensure that the GDPR remains a progressive legislation whose interpretation, implementation

²⁰ UK ICO 2014 Report on Big Data and Data Protection at p. 14, para 49.

and enforcement can evolve as the technology and business contexts evolve. As such, the risk-based approach of the GDPR ensures that the GDPR is technologically neutral and future proof.

PART 2

THE RISK-BASED APPROACH OF THE GDPR IN PRACTICE

In Part 2 of this paper, we discuss the practical application of the GDPR's risk-based approach as part of organisations' accountability and internal privacy management programs. In particular, we examine how organisations can identify, assess and mitigate risks and adverse impact on individuals in a consistent and repeatable manner. We also address other issues and challenges that may arise from the application of the GDPR risk requirements in practice. We propose possible solutions and identify opportunities for further policy development and guidance on key implementation issues.

5. Identifying and Developing an Inventory of Risks and Harms

As discussed above, work has already been done to identify, classify and inventory the risks and harms that might be considered in a risk assessment. To further develop and refine that work for purposes of implementing and applying the GDPR, the following risk assessment elements may be a starting point for a new matrix or categorisation for risky processing activities, threats and harms, based on CIPL's earlier work on risk and its risk matrix, the GDPR's guidance on risky processing activities and harms and further industry input:²¹

5.1 First, the following processing activities qualify as potentially risky processing that may result in harm:

- processing of vulnerable persons' data, such as children's;
- processing of large amounts of data affecting a large number of individuals;
- engaging in a "new kind" of processing or where time has elapsed since an initial DPIA;
- automated processing, including profiling, that provides a basis for decisions with legal effect or similarly significant effect;
- large-scale processing of special categories of data, and criminal conviction and offences data;
- large-scale and systematic monitoring of publicly accessible areas; and
- use of new technologies.

This list of risky processing or "risk triggers" is not exclusive and there may be others that organisations have to consider in each case based on context.

5.2 Second, a risk assessment should consider the potential threats in any given processing. Such threats include:

- unjustifiable or excessive collection of data;
- use or storage of inaccurate or outdated data;
- inappropriate use or misuse of data, including:
 - a) use of data beyond individuals' reasonable expectations;

²¹ CIPL, A Risk-based Approach to Privacy: Improving Effectiveness in Practice, (2014); https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf

b) unusual use of data beyond societal norms, where any reasonable individual in this context would object; or

c) unjustifiable inference or decision-making, which the organisation cannot objectively defend;

- lost or stolen data or destruction and alteration of data; and
- unjustifiable or unauthorised access, transfer, sharing or publishing of data.

5.3 Finally, organisations must assess the likelihood and severity of any harms that might result from the risky processing or threats. Such harms may include:

a) **Material, tangible, physical or economic harm to individuals**, such as:

- bodily harm;
- loss of liberty or freedom of movement;
- damage to earning power and financial loss; and
- other significant damage to economic interests, for example arising from identity theft.

b) **Non-material, intangible distress to individuals**, such as:

- detriment arising from monitoring or exposure of identity, characteristics, activity, associations or opinions;
- chilling effect on freedom of speech, association, etc.;
- reputational harm;
- personal, family, workplace or social fear, embarrassment, apprehension or anxiety;
- unacceptable intrusion into private life;
- unlawful discrimination or stigmatisation;
- loss of autonomy;
- inappropriate curtailing of personal choice;
- identity theft; and
- deprivation of control over personal data.

c) There is no consensus on whether **societal harm** should also be considered in the context of risk assessment and it certainly is not a direct requirement under the GDPR. However, societal harm might be considered as a collection of individual harms in the context of a group of people in a society above and beyond individual harms. This type of risk typically may occur where personal data obtained from businesses is used by governmental bodies. Societal harm also plays a role when data are merely used by businesses, for instance where businesses have such a dominant position that they are capable to impose their values on society. The type of harms may include:

- damage to democratic institutions, for example excessive state or police power; and
- loss of social trust (“who knows what about whom?”).

However, in order to make risk identification and classification in the category of societal harm practicable, objective, measurable and sufficiently concrete, the identified factors will

require proxies or measurable criteria. In addition, it must be clear that any consideration of societal impacts and harms must remain grounded in concrete risk to individuals, which may have wider societal implications. In other words, identifying individual harms must remain a first and necessary step in any consideration of their broader impact in the form of “societal harm”.

Considering **negative impacts to society** may also be consistent with risk assessment in the **context of a legitimate interest** analysis. In such cases, wider factors, such as the interests of (or positive impacts on) relevant “third parties” (including society at large) in a given processing activity may be taken into account according to the WP29.²² In the Google Spain case the EU Court of Justice took as part of the legitimate interest test account of the interest of the general public.²³ This implies that negative impacts and risks to society may logically also be considered.

However, there is a valid concern that it would be difficult for an organisation to articulate and evaluate the societal harms associated with their processing operations. As a result, without precluding organisations to do so where feasible and appropriate, we would recommend that there not be a general expectation or requirement on organisations to determine societal harms unilaterally. In other words, consideration of societal harms in risk assessment may be an area where ongoing dialogue and co-operation between organisations and the DPAs is desirable. In any event, as mentioned above, to consider and assess societal harms, they would have to be more clearly defined, possibly through measurable proxies or criteria, and grounded in individual harms.

- 5.4 Risk may also have a temporal element. Thus, risk can be classified by taking into account the time frame of the impact of the possible harms. From this viewpoint, risks have long-, medium- and short-term impact, which must be considered in any risk assessment.
- 5.5 As mentioned, a risk identification and classification system (with respect to the risky processing activities, threats and harms) is useful as it enables organisations to define the scope of risk management within their organisations and to have a repeatable and consistent framework to identify risks to individuals in multiple scenarios and over time. Indeed, it is crucial that a risk identification and classification system be developed for the GDPR to ensure that organisations have a consistent framework for identifying the relevant risks to individuals raised by their operations and to ensure the effective implementation, interpretation and enforcement of the GDPR provisions on risk. Risk identification and classification for purposes of GDPR compliance is an area that would benefit from further collaborative development and guidance by all stakeholders, including industry and the DPAs.

For purposes of GDPR implementation, it should be possible to achieve a high degree of consistency and agreement in the identification and classification of the relevant risk elements—the “risky processing activities” and threats, as well as the types of harms that might result. This is because such identification and classification will occur within the context of similar practices and shared legal norms and cultural values across the EU.

²² Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC.

²³ Case C-131/12, Google Spain and Google Inc., e.g., at 97.

Similarly, such agreed classification of risk elements might also be possible within certain industry sectors. (In contrast, we do not believe that the actual process or methodology of risk assessment, i.e. how the various risky activities or threats and harms should be weighed and evaluated, can be made similarly consistent across different organisations; rather, the way in which risk is assessed should largely be left to individual organisations. See discussion in Section 7.)

However, even with a widely agreed classification of risks, it should be understood that each organisation has the flexibility and obligation to consider any additional risk elements that are specific to its own context and processing. For many global organisations, such individual contexts might also be impacted by risk classifications necessitated by an organisation's operations in other regions and under other legal regimes and cultural expectations. Indeed, many organisations roll out new products globally without variation between countries. Thus, risk assessments must comprehensively **assess the global impact** of a product. Any further DPA guidance on the elements and methodology of risk assessment must be workable in that context.

6. GDPR: Risk Level, “High Risk” and “Low Risk” Processing

6.1 Determining Risk Level Under the GDPR and Determining “High Risk”

6.1.1 Determining the risk level is essential for the following reasons:

- a) to deliver effective and high-level privacy and data protection for individuals;
- b) to inform the specific mitigations and controls that accountable organisations are required to implement to ensure GDPR compliance; and
- c) to determine whether there is “high risk” that would trigger specific compliance obligations under the GDPR, such as the obligation to undertake a data protection impact assessment (“DPIA”), or to notify individuals of a data breach.

6.1.2 As explained in Section 4.3.1, the GDPR prescribes that the risk level is determined by considering the **“likelihood” and “severity”** of the risks to the individual (taking into account the nature, scope, context and purpose of the processing).²⁴ “Likelihood” means how likely it is that the risk or impact of the risk may materialise. “Severity” means the magnitude of the risk or its impact if it materialises. Thus, organisations must have processes that enable them to reliably and consistently weigh the risks and harms against these criteria in order to comply with the GDPR.

6.1.3 It appears that it will be necessary for organisations to conduct an initial assessment before the DPIA to determine if a DPIA is required. This should be a more light-touch assessment to determine whether certain “trigger” factors are met. Article 35(3)(a) appears to establish certain “default” high-risk categories that require a DPIA under the GDPR, such as:

- the “systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which

²⁴ In the data security context, this includes “state of the art and the cost of implementation.” Article 32(1).

decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person”;

- the “processing on a large scale” of special categories of data; or
- the “systematic monitoring of a publicly accessible area on a large scale”.

A point of clarification on this issue might be whether there is scope and flexibility for organisations to “rebut” the per se “high-risk” status of these types of processing through an initial risk assessment. See further discussion in Section 6.11.

6.1.4 Unlike with the identification and classification of risks where some degree of standardisation and harmonisation is possible, we do not believe that the weighing of risk and risk assessment processes can be similarly made uniform and harmonised across different organisations. We believe any further guidance on the process of risk assessment should recognise that organisations must have flexibility to develop processes that work for them so long as they consider the relevant elements and are able to demonstrate the effective functioning of these processes when asked. This is not to say that high-level guidance that enables some consistency across organisations cannot be developed. See also discussion below in Section 7.

6.1.5 As discussed, the GDPR provides some guidance on what may constitute “risky processing” and what constitutes “high-risk” processing.

The GDPR provisions on the characteristics of “high-risk” processing activities should be regarded as being part of a general risk assessment process rather than the only features to be considered during such a process.

6.1.6 Even where there is suspected or per se “high risk” under the GDPR, in many (if not most instances) the actual risk level (i.e. “likelihood” and “severity”) must be determined on a case-by-case basis by taking into account:

- The nature, scope, context and purposes of the processing; and
- The ability to mitigate a “high risk”, for example in contexts where the absence of such ability would trigger the “prior consultation” requirement under the GDPR.²⁵ This would also be relevant in cases where a processing that initially may be considered a “high risk” is actually downgraded to “normal risk”, based on mitigations and safeguards applied.

6.1.7 The GDPR’s examples of “high-risk” processing include concepts such as “large-scale” processing, “systematic and extensive evaluation” and “systematic monitoring”. The terms “large-scale” and “systematic and extensive” require interpretation. For example, are these

²⁵ Recitals 90 and 94; Article 36.1.

criteria objective or subjective and how can they be further clarified? Moreover, they should be interpreted consistent with the similar provisions in the GDPR's test for mandatory DPO.²⁶

- 6.1.8 In addition, Article 35(1) identifies “using new technologies” as a possible circumstance of “high risk” requiring a DPIA. CIPL does not believe that this should be a stand-alone criteria for triggering “high-risk” categorisation. WP29 guidance on “high risk” should clarify that “using new technology” cannot be the sole trigger for high-risk status or a DPIA, but must be coupled with additional high-risk characteristics, based on context, scope and purpose of processing.
- 6.1.9 Generally, CIPL takes the view that companies should be able to assess themselves whether their processing operations fall within the ambit of the **“systematic-extensive-large-scale” and “using new technology” criteria** using their best judgement and taking into account their whole business operations. Organisations should also be able to identify and demonstrate their decision-making process on this matter in the event of an inquiry or enforcement action by an EU DPA. Thus, WP29 guidance should focus on a set of factors that might be considered to assist companies in assessing whether they fall within the “systematic-large-scale-extensive” criteria.
- 6.1.10 The examples in Article 35(3) of high-risk processing appear to have a per se or default high-risk status for purposes of the obligation to conduct a DPIA, even without an actual prior risk assessment. However, as suggested above, there should be scope or flexibility to “rebut” the presumption through an initial risk assessment, and further clarification of that point would be useful. This approach would also be consistent with our recommendation below in Section 6.2 on the “lists” of high-risk activities to be developed by the DPAs.
- 6.1.11 As mentioned, under Article 35(1) “a single assessment may address a set of similar processing operations that present similar high risks.” Presumably, this provision is intended to avoid unnecessary duplication so that one risk assessment can cover multiple similar scenarios. Any further guidance from the WP29 on DPIAs should clarify that it is the organisations’ responsibility to interpret and apply this provision as appropriate in the context of their own circumstances. However, they must also be able to justify how and why one particular risk assessment was relevant to a set of similar processing operations.

6.2 **“High-Risk” Processing List**

According to Article 35(4) GDPR DPAs are obliged to establish and make public lists with high-risk processing operations that would require DPIA.

- 6.2.1 Difficulties may arise in practice if EU DPAs create fixed or exhaustive lists of “high-risk” personal data processing operations, without making room for context. We take the view that the risk level of personal data processing operations is context specific. The same processing operation may entail significant risk in one context and less risk in another, depending on the organisation’s decisions about how the data are used and how the

²⁶ See CIPL “Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation” (November 2016), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf.

processing is carried out, as well as the risk analysis and mitigation strategy that is employed, and the remaining residual risk.

- 6.2.2 For example, conference and event organisers often collect from attendees their dietary preferences, e.g. vegetarian, kosher, diabetic, etc. This data may reveal sensitive information about individuals' health or religion. Collecting such data should not in itself, however, be considered as "high-risk" processing that would trigger certain GDPR obligations because, in most cases, the data are processed for limited purposes and maintained only for a brief period of time. Moreover, the data are likely not shared with third parties. Thus, it is the context in which such data are processed that may generate "high risks". Similarly, individuals may voluntarily share religious views with certain third parties, including broad or public audiences in the context of social media. In such cases, the voluntary nature of disclosing this information to third parties may mitigate the "risky" nature of processing this data.
- 6.2.3 Another context-related example concerns new technologies and practices. A predefined list will not consider still unforeseen or undeveloped technologies and practices, and a predefined list, in any case, will not be exhaustive. Thus, a list, if there is one, would only be indicative and could not be "final".
- 6.2.4 Article 35(4) of the GDPR asks EU DPAs to come up with a list of "the kind of processing operations" rather than a list of specific processing activities. Hence, this provision of the GDPR may be interpreted more broadly to call for a list of examples of processing operations that can be coupled with additional criteria that organisations can then subject to a risk assessment process to make context-specific determinations on whether a specific processing operation is a high-risk activity.
- 6.2.5 In other words, the list of "the kind of processing operations which are subject to" DPIAs, could be a list of specific features, criteria and characteristics of personal data processing activities that may be considered "high risk". Once a personal data processing falls within the ambit of the "high-risk" list, the organisation can then determine the actual risk level of the processing operation through a risk assessment, taking into account all the relevant factors, including context, purpose and scope of processing. This approach would make sense given that Recitals 76 and 84 of the GDPR specify that organisations must be able to determine "high risk" by using a risk assessment process.
- 6.2.6 Another appropriate solution that would be in line with the GDPR and be context specific would be for any EU DPA guidance on "the kind of processing" that is subject to DPIAs to create **rebuttable presumptions** of processing that is "high risk". This would mean that such "lists" would include examples of activities that are deemed presumptively "high risk", unless proven otherwise by the organisations via an appropriate risk assessment and/or appropriate mitigations. Note, however, that absence from such "high-risk" list should not create a negative inference that the criterion or activity is necessarily "low risk" (see below).
- 6.2.7 Under both options, prior consultation with stakeholders would be helpful before the DPAs release final additional "high-risk" guidance. It is also paramount that there be consistency across such lists and further guidance by the EU DPAs.

6.2.8 Figure 1 below illustrates the options for further guidance on “high risk”. As indicated above, CIPL recommends the approaches set forth in the two columns on the right for future WP29 guidance.

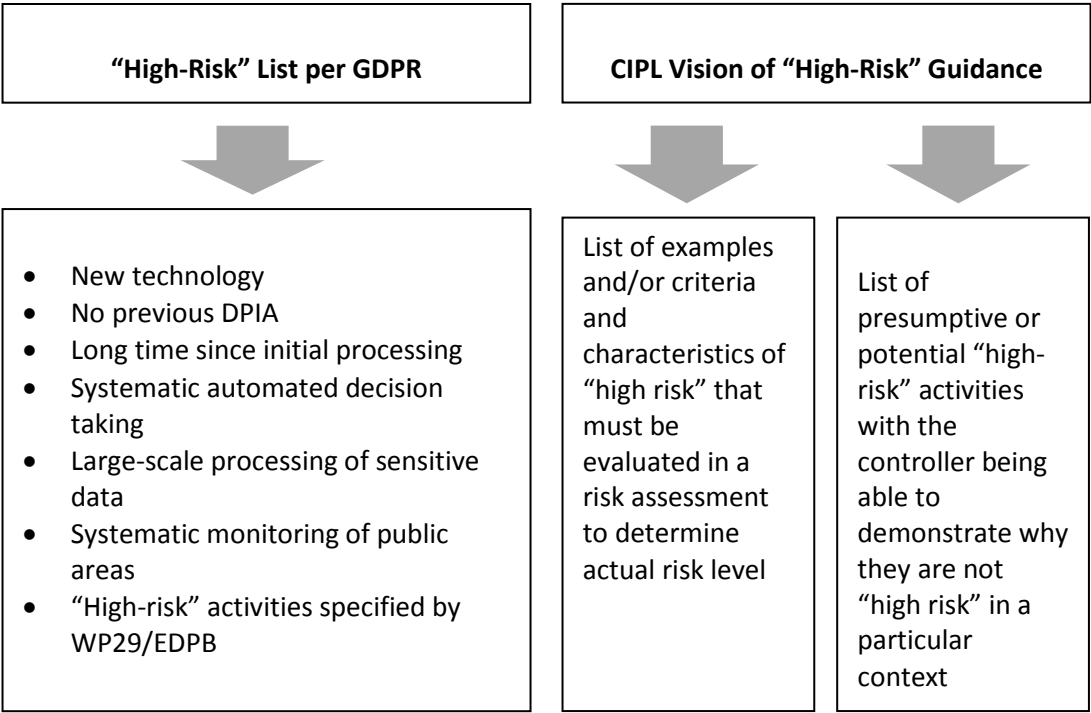


Figure 1: Guidance on “High Risk”

6.2.9 Table 4 below sets out a non-exhaustive list of additional criteria, characteristics and examples of “high risk” which could be used to determine “high risk” in the model described above.

Examples, Criteria and/or Characteristics of “High Risk”	
1	Scope of material and non-material damage (e.g. individual, population of relevant individuals or society generally)
2	Impact of material and non-material damage (e.g. individual, population of relevant individuals or society generally) (keeping in mind that intangible, non-material harms may often be considered lower risk than material/tangible/physical harms)
3	Volume of personal data processed
4	Number of individuals subject to processing
5	The number of parties (e.g. third parties and employees) accessing the data
6	The type and number of third-party recipients

7	Geographical spread of processing activities
8	Processing multiple data sources
9	Type of personal data processed — e.g. sensitive personal data or personal data regulated by other laws (health, financial, biometrics)
10	Length and frequency of data processing
11	Processing of data collected from individuals (“original” personal data) or data derived, observed, inferred about individuals (“secondary” personal data)
12	Retention period of the data

Table 4: Examples, Criteria and/or Characteristics of “High Risk”

6.3 “Low-Risk” Processing Lists

6.3.1 As mentioned earlier, the GDPR also allows EU DPAs to establish lists of processing where no DPIA is required, presumably because there is “low risk”.

We believe that establishing criteria, examples or lists of processing where no DPIA is required (because of “low risk”) will be very helpful to organisations. As with “high-risk” lists, absence of a criterion or activity from the low-risk list should not create an inference that it is “high risk”.

One example of a low-risk activity on such a list could be the processing of employee data to fulfil the rights and obligations in an employment relationship. Most national laws, in fact, exempt such processing from prior notification requirements, which suggests a recognition of low risk. Moreover, to the extent DPAs have already characterised certain processing activities as common, frequent or low risk, such as HR data and customer relations data, any future guidance on low risk should be consistent with such earlier guidance.

6.4 Requiring DPIAs for “High-Risk” Processing Activities

6.4.1 Regarding DPIAs generally, current practice suggests a two-stage process.

- a) The first process is a screening process or initial risk assessment to determine whether there is “high risk” requiring a DPIA, which will need to be completed prior to any new processing.
- b) If the screening process indicates that a DPIA is needed then this leads to the second process, which is a full-blown DPIA, as required by GDPR. This also includes a risk assessment as well as controls to comply with the requirements of data protection by design under the GDPR.

6.4.2 The following diagram shows the stages of risk assessment under the GDPR²⁷:

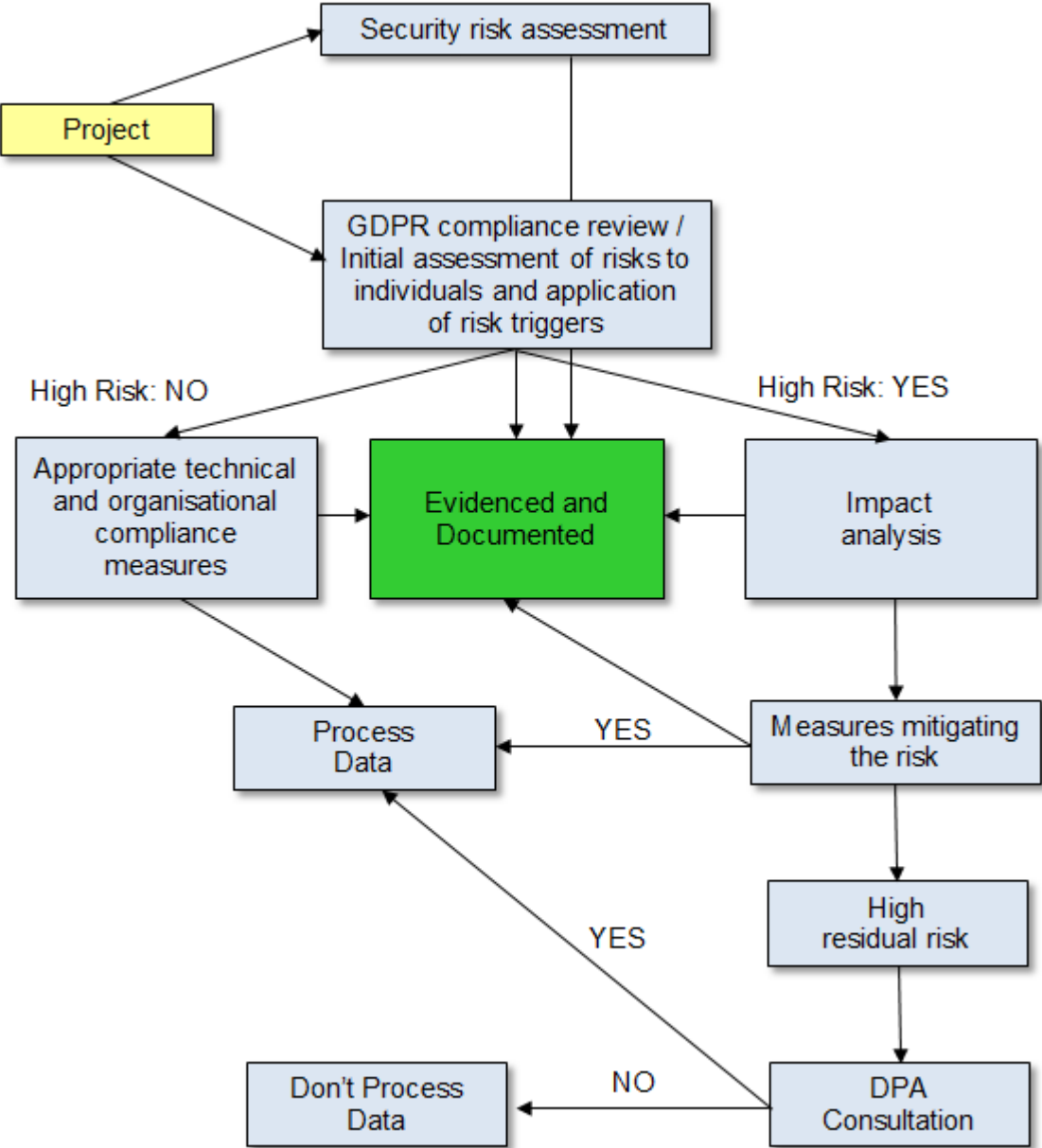


Diagram 1: Stages of Risk Assessment

²⁷ Note that while the diagram places the consideration of mitigations in the Data Protection Impact Assessment, the mitigations could also be considered in the initial assessment, thereby potentially avoiding the need for a DPIA. See Section 6.4.3.

6.4.3 A point of clarification by way of further guidance and stakeholder input may be the issue of how to distinguish between the initial risk assessment or screening process to determine the need for a DPIA and the risk assessment component of a DPIA. For example, does the initial risk assessment or screening process consider mitigations and residual risk? If so, how does the prior consultation requirement under the GDPR work since it requires consultation with the DPA if the DPIA shows that a high risk remains after mitigations have been applied? It appears that such inability to mitigate out of high risk would already be evident in the initial risk assessment, if that assessment included mitigations and the assessment of residual risk.²⁸ There is likely to be a balance in each organisation between the level of detail in the initial assessment and the number of processing activities which need a full DPIA: if the initial assessment is quite detailed, then fewer activities will need a full DPIA, and vice versa. There will be advantages and disadvantages to either approach, depending on, for example, the resourcing available.

6.5 **Prior Consultation**

6.5.1 It follows from Article 36(1), as explained in Recital 94, that where a DPIA indicates that the processing would result in high risk in the absence of mitigation measures and the controller, in its opinion, cannot mitigate the risk by reasonable means in terms of available technologies and cost of implementation, the controller must consult with the EU DPAs. This reading raises several questions. For example, the GDPR assigns responsibility to the controller to determine whether the trigger for consultation—the inability to mitigate with “reasonable means”—is met. However, the GDPR does not specify the subject of the consultation. Thus, it would be helpful to clarify whether the consultation will be about (a) the accuracy of the controller’s assessment that the high risk cannot be mitigated and/or (b) whether to proceed with the processing despite these high risks, for example when there is a substantial benefit.

6.5.2 In our view, it appears that the prior consultation requirement of GDPR de facto amounts to prior authorisation. To avoid overburdening both the organisation and the DPAs, we believe that prior consultations and authorisations should be the exception rather than the rule and reserved for special circumstances and limited cases.

6.5.3 At the same time, it would be helpful for WP29 to recognise the need to maintain the ability for organisations and their DPOs to seek informal consultations and ongoing dialogue with DPAs, in addition to formal prior consultations. Experience shows that such informal consultations yield positive outcomes for both the organisation and DPAs, help resolve issues in a collaborative manner and foster trust. Such informal consultations are also consistent with the tasks of the DPO to co-operate with the DPA under Article 39(1)(d) and to consult with the DPA on any matter under Article 39(1)(e). Finally, the GDPR’s concepts of “one-stop-shop” and lead authority are very much predicated on the ability of the organisation to work more closely with a lead DPA and the lead DPA to have deeper involvement and knowledge of the organisation’s business model and processing operations.²⁹ Informal consultations would be an integral part of that relationship with the lead DPA. Keeping in mind issues of

²⁸ See Article 36(1) and Recital 94.

²⁹ See also the CIPL Paper of 30 November 2016 on the One-Stop-Shop and the Lead DPA as Co-operation Mechanisms in the GDPR, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_the_gdpr_one-stop-shop_30_november_2016.pdf

overburdening the DPAs and the fact that such informal consultations are not mandatory, we believe that having the ability for informal, efficient and not overly regulated consultations, especially with the lead DPA, should be preserved as benefiting both the organisation and the DPAs. This is an area where additional guidance clarifying the DPA's expectations and capabilities would be helpful.

7. Risk Assessments in Practice

7.1 Methodologies for Risk Assessments — General

- 7.1.1 As discussed, the GDPR effectively requires organisations to conduct risk assessments in various contexts, including DPIAs, breach notification, privacy by design, etc. Accordingly, organisations will have to devise effective, repeatable and appropriate risk assessment methodologies that incorporate certain generally agreed-upon risk factors and considerations that are flexible enough to be adaptable to specific data processing contexts. This task is likely to be spearheaded by the organisation's DPO or other appropriate function.
- 7.1.2 Because the GDPR distinguishes between different risk levels and associated obligations, it may invite the perception that the relevant assessment processes might be different for the different risk levels as well. However, the general risk assessment elements, factors and considerations, as well as the processes or methodologies for such risk assessments, must be the same for all instances in which risk assessment needs to be carried out and for all categories of risk (low, medium and high risk), as the actual level of risk can only be known at the end of the assessment process. Nevertheless, this does not suggest that a single risk assessment methodology needs to be selected and applied for all types of risks within the same organisation. The same methodology should be used for comparable processing operations in order to produce comparable results on the level of risk.
- 7.1.3 However, we do not believe that risk assessment processes or any weighting or scoring methodology can or should be made uniform, one-size-fits-all and harmonised across different organisations. Instead, it should be **principles based and adaptable** to specific organisations, businesses and contexts.
- 7.1.4 To the extent model methodologies are developed, they might include examples of data protection/privacy risks, threats, damages and harms to consider (including those addressed in this paper), as well as questions that organisations could consider as they evaluate the risks of their proposed processing activities. This approach will help to ensure that organisations can successfully apply the relevant high-level data protection principles and obligations to their specific circumstances.
- 7.1.5 **Particular sectors** (e.g. health, banking, etc.) could use such principles-based methodologies to develop sector-specific guidance if needed to reflect the specificities of their sectors. However, such sector-specific guidance should also not be too prescriptive and should give organisations the necessary latitude to adapt the methodology for their own contexts.
- 7.1.6 Nevertheless, there is scope for further high-level and general guidance on the risk assessment process and methodology (including for purposes of the DPIA context; see below). CIPL may develop more specific recommendations on the specific issue of process and methodology in the future.

- 7.1.7 Finally, in developing any further guidance on risk assessment methodology and process, it may be advisable to consider the more mature risk management methodologies and processes of other industries, such as in the environmental and financial fields.

7.2 Risk Assessment Methodologies in the Context of DPIAs

- 7.2.1 DPIAs are a specific and perhaps the most recognisable example of a risk assessment that organisations will have to perform in respect of high-risk processing. Indeed, many organisations already perform more or less formal PIAs as a matter of best practice and accountability. However, as discussed above, the GDPR requires many other instances of risk assessment beyond DPIAs, such as in the context of data breach, privacy by design, legitimate interest, etc.
- 7.2.2 It is likely that some of these assessments may be combined or merged into a DPIA. For example, it is likely that consideration of risk in the context of privacy by design would be part of a DPIA. Equally, when a controller needs to determine a lawful ground in respect of a new application and new processing of customer or employee data and perform a risk assessment if the legitimate interest ground is considered, then that risk assessment would be an integral part of privacy by design and the DPIA in respect of that new application or new processing.
- 7.2.3 In other instances these assessments will be separate. For example, a security or privacy incident may result in a high-risk data breach that will have to be notified to individuals (in addition to DPAs). The assessment of the level of risk and harm to individuals in that context is quite separate and different from a DPIA that may have been performed for the underlying processing that subsequently experienced the security breach.
- 7.2.4 The GDPR provides minimal guidance on the risk assessment process, providing only that it must assess the likelihood and severity of risks, taking into account the nature, scope, context and purposes of the processing. The same is true with respect to risk assessments in the context of a DPIA, though Article 35(7) of the GDPR provides some guidance and specific steps and requirements for performing DPIAs: The DPIA must contain a systematic description of the processing operation, its purpose and, where applicable, the legitimate interest that is being pursued. It must also include an assessment of the necessity and proportionality of the processing in relation to its purpose, as well as an assessment of the risks to the rights and freedoms of the data subjects. In addition, it must include the relevant mitigation measures and safeguards, taking into account the rights and legitimate interests of the affected individuals.
- 7.2.5 It may be helpful to consider the relevance of the above specific DPIA requirements for general, non-DPIA risk assessment methodologies, as well as to examine existing PIA risk assessment methodologies and practices for purposes of devising further guidance on general risk assessment methodologies, again, keeping in mind the question of whether and to what extent risk assessments, including DPIA risk assessments, should ever be templated rather than remain organisation and context specific. Importantly, some DPAs have issued

DPIA guidance already, such as the UK, Spain and the CNIL.³⁰ These are helpful as guidance in helping organisations create their own risk assessment processes.

- 7.2.6 Going forward, it is important that any guidance remain flexible. The more complex the expectations and guidance in respect of DPIAs, the more likely organisations will interpret “high risk” narrowly in an effort to avoid burdensome and formal DPIAs. Yet DPIAs are important tools and organisations should be incentivised to use them and embed them in their day-to-day processes.
- 7.2.7 Article 35(9) on DPIAs also provides that, “where appropriate”, organisations should also seek “the views of individuals or their representatives”. This may be problematic for private sector organisations, as it may undermine their commercial secrets and IP rights. Also, some organisations have no direct relationships with individuals. Organisations should be allowed some flexibility in how and in what circumstances they implement this requirement, especially where it may run contrary to their legal rights and commercial interests. For example, there may be an opportunity for some privacy “feedback” as part of any product roll-out in “developers’ version” mode prior to formal roll-out. Otherwise, we believe that this requirement may be better suited for public sector organisations, where there is already an existing practice of wider consultation of the general public in respect of PIAs carried out by public sector bodies.

7.3 Other Considerations and Requirements for GDPR Risk Assessments

7.3.1 Benefits of Processing

Risk assessments of processing operations must take into account the **benefits of processing** to multiple stakeholders, such as the individual or group of individuals, organisation(s) and society. Because any risk assessment must begin with a clear statement or description of the contours and purpose of the proposed processing, consideration of the benefits must also come at the beginning, given the close relationship between “purpose” and “benefits” of a given data processing activity.

Indeed, the GDPR explicitly requires the consideration of “purposes of processing” in connection with risk assessments. Thus, in the context of the DPIA requirements, Article 35(7) suggests that any evaluation must take into account the proportionality between risk/harm and the purposes, interests or benefits that are being pursued. This indicates that the ultimate assessment of risk is relative to the ultimate assessment of purpose, interest or benefit. In other words, a case in which the purpose of the processing includes significant benefits and “legitimate interests” of the controller or third parties, the proportionality calculation may be different from where there are no such benefits or interest. This, of course, is common sense, but we believe that future guidance should clarify that.

³⁰ UK ICO, “Conducting privacy impact assessments code of practice” (February 2014); Spanish DPA, New Guide on Impact Assessments on Protection of Personal Data, (October 2014), http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf; CNIL, Privacy Impact Assessment Methodology (2015), Tools (2015) and Good Practices (2012), <https://www.cnil.fr/en/rights-and-obligations>.

In its opinion on “legitimate interest”, the WP29 discusses the close relationship and partial overlap between the concepts of “interest”, “purpose” and “benefits”, pointing out that the “interests” or intended benefits of a processing activity might include benefits to the organisation (or third parties) or to society.³¹ Indeed, the “legitimate interests” of a “third party” in Article 6(f) of the GDPR includes the interests of individuals and society, i.e. benefits to individuals or broader societal benefits. This is also made clear in the WP29’s above-referenced opinion on legitimate interest.³²

The reason that the benefits or purposes of processing should normally be considered at the outset of a risk assessment is to avoid the unwitting or unnecessary reduction of the benefits of processing, especially when the benefits are clear and positive for all the relevant stakeholders. A good example of such loss of benefits is reduced user functionality or a less efficient customer experience when a website operator would be precluded from providing an option to store payment card data for future purchases or an organisation prevented from sharing data internally so that customers do not have to repeatedly answer the same questions throughout a service.

Equally, risk assessment in the context of the GDPR needs to ensure that in preserving the benefits they do not disproportionately impact negatively on the individuals and their fundamental rights and freedoms.

Figure 2 illustrates a risk assessment process in all of its stages, including the consideration of the benefits of personal data processing operations:

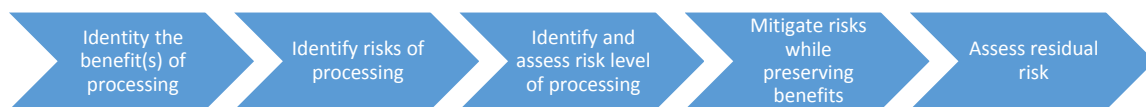


Figure 2: Risk Assessment from a Purposes Perspective

7.3.2 Reticence Risk Consideration

Further, a risk assessment might consider the failure to pursue certain purposes, interests and benefits in term of the risks and potential harms of not pursuing them. This is called the “**reticence risk**” or the risk of not engaging in processing that would bring about benefits to various actors. Instead of asking “what will we (or third parties) gain from this processing activity?” organisations would be asking “what will we (or third parties) lose if we don’t pursue this processing activity?” However, while this is related to the question of benefits, it is not the same, as it measures the cost of inaction, which is not merely the converse of the potential benefits but also includes any additional harms besides the harm of not getting the benefit.

The textual support in the GDPR for considering reticence risk as part of a risk assessment is similar to the support for considering “purpose”, “interests” and “benefits” as overlapping

³¹ Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC at pp. 23-24

³² *Id.* at 24.

and related concepts, as discussed above. Where the interests of a controller or third parties may be considered in a risk analysis, their interest in not incurring a loss or damage must be considered. We would encourage guidance that makes it clear that reticence risk may legitimately be considered. Of course, as with all other factors to be considered, we believe an organisation should be able to demonstrate how and why they were considered and how the consideration impacted the outcome of the risk analysis.

7.3.3 Responsibility for Risk Assessments and Decisions Based on Risk Assessment

The DPO has an implicit obligation to advise in respect of DPIAs. However, this does not mean that the DPO must carry out DPIAs by himself or herself or be exclusively responsible for it. It is likely that others in the organisation will carry out preliminary pre-screenings or risk assessments and then escalate complex or high-risk matters to the DPO.

As an example, in order to understand the risk of a data breach for the purposes of notification to EU DPAs, a risk assessment can be undertaken by the DPO, Chief Information Officer (CIO), Chief Information Security Officer (CISO) or computer incident response and forensic teams in the organisation. This may vary across organisations. In some organisations, it may very well be the case that the DPO is the main function responsible for all types of risk assessments. CIPL does not believe that this is a sustainable approach in the long term. Rather, CIPL would recommend risk assessment tasks be delegated across the organisation, as appropriate. The role of the DPO would then be to define high-level guidelines or methodology, to serve as a second-tier reviewer or a point of escalation, and to ensure monitoring and evidencing of the DPIAs and their outcome. Thus, due to the potentially distributed nature of risk assessments, risk assessment methodologies should be **easy to understand and easy to use** by experts and non-experts from various parts of an organisation, including IT, marketing, HR, data scientists, privacy engineers, etc.

Organisations, via the DPOs, must also promote **management buy-in** for risk assessment and **embed it** within their organisations in all functions and especially in the development of their products and services that rely on processing of personal data. In fact, it is likely that a DPIA and other types of risk assessment would be integrated in the organisation's other processes, such as product development and review, sign-in for new technologies and systems, merger and acquisition due diligence, vendor due diligence, etc.

A separate but related issue is who within an organisation draws conclusions from or makes the decisions based on the risk assessment or DPIAs. Thus, while the risk assessment will result in a finding of risk or of residual risk after mitigations, decisions will have to be made about what mitigations to implement, or, at the end of the process, whether to proceed with the processing operation in light of the residual risk. Both the decisions about mitigations and whether to proceed in light of any residual risk likely will have to involve management in consultation with the DPO. In the case of disagreement, the issue will have to be raised with the "highest level of management" under the GDPR.

8. Risk Mitigation and Residual Risk

There are numerous ways to mitigate risks, some of which are referenced in the GDPR. For example, the GDPR refers to various risk mitigation measures including encryption, pseudonymisation, anonymisation and participation in codes of conduct or certifications and seals. The recommendations set forth in this paper might be incorporated in such codes of conduct or certifications and seals.

In addition, organisations can adopt other mitigating measures depending on the context in question. Examples of such measures include: limiting access and data sharing; limiting use by third parties; limiting geographical scope; restricting subsequent processing; enhancing transparency; implementing new or enhanced security measures, more diligent choice of processor, closer third-party management; training employees involved in risky processing; deciding not to collect or store particular types of data; limiting retention periods; ensuring secure and permanent personal data deletion; developing and/or using systems which allow individuals to access their personal data more easily; developing and/or using systems that make it simpler to respond to data subject access requests; taking steps to ensure that individuals are fully aware of how their personal data are used and can contact the organisation for assistance; selecting data processors that will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf; producing data-sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with; and numerous other specific compliance and governance controls that address the specific nature of the identified risks.

As is evident, there are a host of mitigation measures and safeguards which organisations can implement to protect individuals and minimise risks to them. The crucial issue here is selecting the right mitigation measures, taking into account the context in question. Consequently, choosing appropriate mitigation measures should be done on a case-by-case basis. The preference for case-by-case should be included in any future DPA guidance on mitigations. This guidance should specify that organisations will have to consider the risks involved, the cost of implementing the measures and effectiveness of these measures, as well as their impact on the purposes, interests or benefits that are being pursued by the proposed processing activity. Considering the appropriate mitigations also requires taking into account the reasonable expectations of individuals, transparency and the elements for fair processing.

CIPL emphasises that mitigation does not mean complete elimination of risk. It means reducing or minimising risk to the greatest extent reasonable given the desired benefits and reasonable economic parameters. (Note that "cost of implementation" of security measures is an appropriate consideration under Article 32.) At the end of the process of assessing the risks and implementing mitigations, the organisation likely will be left with some residual risk and will have to decide whether to proceed with the processing in light of that risk. An open dialogue and ability to consult DPAs informally may help organisations make these decisions.

Organisations will have to make a defensible decision about whether to proceed with data processing in light of any residual risks. In making that decision, the issue of "proportionality" vis-à-vis purposes, interest and/or benefits will have to come into play, as discussed above. Also, in appropriate contexts, organisations may be able to legitimise processing of data and acceptance of the residual risk by seeking fully informed and explicit consent of individuals.

9. Demonstrating Compliance with the GDPR Risk Assessment Requirements

The GDPR requires that controllers implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. Thus, where organisations are required to conduct risk assessments or DPIAs as part of their GDPR compliance obligations, they must also be able to demonstrate that they have conducted such risk assessments or DPIAs.

Consistent with the basic elements of organisational accountability, this requires that organisations evidence, document and maintain records of their risk assessment processes and decisions. Apart from enabling and streamlining internal operations and decision-making, this will enable them to demonstrate to the EU DPAs that they have a risk assessment process in the first place, that they have carried out the risk assessment process for the specific processing operation, and that the process is adequate for the purposes of the GDPR. Indeed, multiple GDPR provisions, such as those relating to legitimate interest processing, breach notification and use of certifications to demonstrate compliance with relevant provisions, underscore the obligation to create and maintain verifiable and demonstrable proof of risk assessments in the event of internal or external audits or investigations by the DPAs.

10. GDPR Risk Assessments and EU DPAs

In order to fulfil their GDPR tasks, CIPL suggests that EU DPAs should also apply the risk-based approach and be able to undertake risk assessments in the performance of their own statutory obligations. DPAs, especially the lead DPA, should maintain an ongoing dialogue with organisations, which, in turn, is key to ensure that DPAs fulfil their tasks in full knowledge of the impacts of their decisions and to ensure maximum efficiency of their role without unnecessary impacts on businesses.

EU DPAs must be able to review and evaluate the risk assessments, including DPIAs, conducted by organisations, when they exercise their investigative and corrective powers under Article 58 GDPR and in the handling of complaints. This will not necessarily require a *de novo* risk assessment by the EU DPAs. However, EU DPAs must be able to understand and evaluate the risk assessment process of the organisation and assess whether the organisation undertook the risk assessment in compliance with its GDPR obligations. The relevant questions for EU DPAs in this context include whether the organisation:

- a) Acted reasonably when undertaking the risk assessment, having regard to all relevant circumstances;
- b) Has risk assessment policies and procedures which enable this process to be carried out by the organisation on a systematic and repeatable basis; and
- c) Has conducted the risk assessment and DPIA process diligently and reached a reasonable conclusion at the end of the risk assessment. This protects organisations from the uncertainties inherent in a flexible process by allowing for different conclusions and results so long as they are well founded, in line with GDPR requirements and have a firm evidentiary basis.

CIPL also believes that EU DPAs should adopt a risk-based approach to their supervisory and enforcement roles under the GDPR. The activities of EU DPAs in all cases should be proportionate to

the risks a specific personal processing operation posed to the fundamental rights and freedoms of individuals. This does not mean that EU DPAs do not have to comply with their specific GDPR obligations, such as investigating complaints filed by data subjects. However, having a consideration of risk enables EU DPAs to prioritise their tasks according to the risk level posed by a processing operation.

The same principle should apply to fines, where the level of risk should be one of the factors in the application of the fine.³³ High-risk violations should entail higher fines than low-risk violations. In these instances, EU DPAs may have to make de novo risk assessments because they will not always have access to or be able to rely on existing risk assessments by the organisation. Article 83(2)(a) supports this interpretation as it requires DPAs to give due regard to the “gravity of the infringement” by taking into account, among other factors, “the level of damage suffered”. The assessment of gravity and damage implies the consideration of risks and harms to individuals and will require a DPA to conduct the risk assessment in a particular case.

Further, CIPL believes that it would be beneficial for EU DPAs to articulate a risk-based approach to enforcement to increase the predictability of regulatory enforcement and motivate better and more targeted compliance responses by organisations. Specifically, CIPL suggests the EU DPAs describe in their enforcement guidelines how they will apply the risk-based approach to make the enforcement policies transparent.

The regulatory approaches by DPAs will be part of a separate paper of CIPL.

11. Conclusion

If implemented with sufficient flexibility, the risk-based approach will play a vital role in ensuring that the GDPR remains technology neutral and future proof and thus capable of delivering effective privacy data protection to individuals in the long run. This is because rather than creating one-size-fits-all rules and obligations that soon may be outdated, the risk-based approach provides for a process with outcomes that can change with context and adapt to changing technologies and business practices. Thus, decisions about whether and how to proceed with certain processing operations will always be tailored exactly to the circumstances and thus more likely to be appropriate for the protection of the rights and freedoms of individuals. Such context-specific solutions are prerequisite for facilitating and ensuring technological and business innovation and societal progress on the one hand, as well as protecting individuals on the other. This risk-based approach will also be most effective from both a protection of fundamental rights and a business standpoint if there is an ongoing and open dialogue between organisations, DPAs and law and policymakers about the constantly evolving technologies and business practices as well as the needs and expectations of individuals and society. The suggestions and recommendations in this paper are intended to maximise this promise of the risk-based approach. We welcome any further engagement on this issue as all relevant stakeholders continue along the path of GDPR implementation.

³³ See Article 83.2

APPENDIX I -- Examples of Existing Sources on Risk Management

US Computer Matching and Privacy Protection Act 1988, 5 USC § 552a(o).

Article 29 Data Protection Working Party, [Opinion 03/2014 on Personal Data Breach Notification](#), 693/14/EN WP 213 (2014), 4.

[E-Government Act of 2002](#) (requiring PIAs for US federal government agencies).

UK Information Commissioner's Office, [Conducting Privacy Impact Assessments Code of Practice, 2014](#) (Guidance).

New Zealand Privacy Commissioner, [Privacy Impact Assessment Toolkit, 2015](#) (Guidance).

[Australia Guide to undertaking privacy impact assessments, 2014](#) (Guidance).

Article 29 Data Protection Working Party, [Statement on the role of a risk-based approach in data protection legal frameworks](#), 14/EN, WP218 (2014), 2.

Data Protection Directive 95/46/EC requires that security measures must “ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected” (Article 17); that “processing operations likely to present specific risks to the rights and freedoms of data subjects” be subject to “prior checking” by member states (Article 12); that personal data may be processed when “necessary for the purposes of the legitimate interest pursued by the controller or by the third party or parties to whom data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subjects ...” (Article 7(f)); and that access rights to data processed for scientific research may be limited “where there is clearly no risk of breaching the privacy of the data subject.” (Article 13(2)).

Organisation for Economic Co-operation and Development, [Supplementary Explanatory Memorandum to the Revised Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data](#) (2013), 30.

Commission Nationale de l'informatique et des Libertés, [Methodology for Privacy Risk Management](#) (2012), 4.

Federal Trade Commission, [Protecting Consumer Privacy in an Era of Rapid Change](#) (2012), 30.

National Institute of Standards and Technology (NIST) Internal Report 8062 (DRAFT), Privacy Risk Management for Federal Information Systems, May 2015,
http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf.

Guidance on Risk Analysis Requirements under the HIPAA Security Rule,
<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf>.

Note that the breach notification laws of 36 US states require a risk of harm analysis.