GDPR DPIA: should it be illustrated with a risk matrix, and if so, which one?

By Bruno RASLE
bruno_rasle@halte-au-spam.com

Paris, 20 March 2026

Impact assessment is one of the major advances of the GDPR and a powerful lever for ensuring compliance with processing that may pose high risks to data subjects. It is also one of the most complex tasks that data controllers, under the guidance of their DPO, approach with caution – even apprehension. The exercise takes the form of a deliverable submitted to the controller for approval and decision-making, in particular to ensure that risk management measures are operational before processing begins. Although not required by the GDPR, it has become customary to illustrate this document with a risk matrix. Is this a good idea? What are the objectives of including it? How should it be designed and how should the feared events and the associated gross and residual risks be positioned within it? Are there any pitfalls to avoid, biases or limitations to this approach? And what are the characteristics of a "good" risk matrix in the context of a formalised PIA under the GDPR?

Privacy Impact Assessment is one of the major advances of the GDPR (along with data breach notification) and a powerful lever for ensuring compliance in processing operations that are likely to pose high risks to data subjects. It is also one of the most complex tasks, which data controllers approach with caution – even apprehension – under the guidance of their DPOs. The impact assessment takes the form of a deliverable that should be submitted to the controller for approval. It has become customary to illustrate this document with a risk matrix. Is this a good idea? What are the objectives of including it? Are there any pitfalls to avoid? And what are the characteristics of a "good" risk matrix in the context of a formalised DPIA under the GDPR?

The author presented this work on Friday, 20 March 2026 as part of the AFCDP University of the DPO 2026.

The DPIA is undoubtedly one of the most powerful tools at the disposal of the DPO[1]

As I indicated in my September 2022 article entitled "Do you have to be paranoid to do a good PIA? ", the obligation in certain cases to carry out a *Data Privacy Impact Assessment* (DPIA) is, in my opinion, one of the most powerful tools available to a DPO to lead their organisation on the path to compliance, although this is by no means an easy task[2] . And within this exercise, there is one that presents its own challenges: producing a risk matrix that offers "*a simplified approach to reality that is easily understandable by all*," as Raphaël De Vittoris and Sophie Cros point out in their book *Déjouer les risques* (Dunod, 2024). How can we achieve synthesis and visual clarity when dealing with the complex abstraction that is risk? This is the subject of this paper.

Why enhance a PIA with a visualisation of risks?

Article 35 of the GDPR does not require any representation of risks to be included in a DPIA, and the guidelines on data protection impact assessments issued by the Article 29 Working Party (WP 248 rev. 01, amended and adopted most recently on 4 October 2017) do not even address this issue. It should also be noted that the teleservice published by the Spanish authority and the template made available on by the ICO do not include any illustrations, even though the latest DPIA published by the British authority does include

[1] The DPO "oversees" the completion of a DPIA, but is not responsible for "doing" it.

[2] See "*Five versions of PIA/AIPD before getting it right*", Bruno Rasle, August 2024. Although the impact assessment is *primarily* an internal document, it may be requested by external auditors (and by the CNIL as part of an inspection), which means that great care must be taken when drafting it.

some, such as the one on the processing associated with CoPilot[3] . I must admit that I found the DPIA carried out on behalf of the Dutch Ministry of Justice and Security on Microsoft 365 laborious (not to say indigestible) to read: the analysis comprises more than 130 pages of text. It is not until page 127 that we find a single 3x3 matrix showing the gross risks (surprisingly, the document does not present any matrix showing the net risks[4]). The same is true of the "*Microsoft 365 Copilot DPIA*" published at the end of 2024 by the same ministry, which comprises 183 pages. Most of the measures for dealing with the identified risks are to be implemented by Microsoft. Does this mean that the author of the DPIA did not want to take their implementation for granted?

To encourage my fellow DPOs to include an illustration that visualises the risks and their level within a GDPR impact assessment, I could quote from my March 2020 article entitled "*DPO colleagues: The annual review is a valuable tool – Let's make it a best practice*", in which I addressed the following question: *"Can my report be illustrated?*" Here is the extract in question, which can easily be applied to our subject: "*The document must be designed to be read and understood by the data controller. Here are some recommendations concerning the content and form of a report intended to be read, understood and used by management on a topic similar to that of compliance: IT security. They are taken from the book "La fonction RSSI" (The RSSI Function), written by Bernard Foray, a member of the AFCDP: "Think KISS (Keep it Simple & Stupid), Pay attention to semantics, Think Comparison (both internal and external), Think Duration and Context, Think Visual-Sales-Sexy.*"

The graphical representation of risks is therefore primarily an internal communication tool, which serves as a visual aid during meetings with stakeholders[5] , aiming to present a summary of the feared events and to assess their consequences in relation to their probability of occurrence. This matrix is primarily intended for the data controller, to whom the impact analysis will be submitted for signature, as it facilitates understanding (in support of the text), as recommended by NIST[6] in its document *Guide for conducting Risk Assessment*: *"Task 3-1: Communicate and share the results of the risk assessment with the organisation's decision-makers to support the measures taken to respond to it. The objective of this step is to ensure that decision-makers have the appropriate risk information necessary to inform and guide their risk decisions. Organisations can communicate the results of the risk assessment in a variety of ways (e.g., executive briefings, risk assessment reports, dashboards).*" I have only found the Office of the Privacy Commissioner of Canada, in its guide on Privacy Impact Assessments (PIAs), to recommend, among its "best practices," the use of visual tools such as tables or diagrams.

Depending on its type, characteristics and quality (and as part of a GDPR impact assessment), illustrating the risks can also highlight important points, showcase the work carried out (by showing the transition from gross risks to net risks[7]) and facilitate the monitoring of the action plan, for example by assigning a pilot for each risk[8] , verifying the proper implementation of processing measures, creating indicators or enabling reviews or audits to be scheduled. It may also be one of the only pieces of information read by the data

[3] "*Data Protection Impact Assessment (DPIA) – Microsoft CoPilot 365*", ICO, Draft, 2024

[4] The Dutch Ministry of Justice and Security seems to have evolved on this issue because, in December 2025, it published a framework for assessing the quality of DPIA produced within entities attached to the ministry. With regard to the risks for data subjects, the level to be achieved is described as follows: "*All risks are described on the basis of realistic scenarios. A risk matrix listing the risks is included. Gross and net risks are clearly indicated.*"

[5] See "*Improved communication: A clear and structured risk register promotes better communication and collaboration among stakeholders, ensuring that everyone understands the organisation's risk landscape*" in *NIST SP 800-30 Guide for conducting Risk Assessment* - September 2012

[6] *National Institute of Standards and Technology*

[7] In this document, I use the term *gross risk* to refer to risk before any treatment (more rarely, we encounter the terms *inherent* or *intrinsic*) and the terms *residual risk* or *net risk* to refer to the risk remaining once all risk control measures have been implemented. During my training courses, to illustrate the difference between the two concepts, I ask the following question: "*If you were given the choice, which amount would you prefer to see deposited into your bank account at the end of each month? Your gross salary (before any deductions) or your net salary?*"

[8] The inclusion of "risk owners" among stakeholders is also found in the Ebios RM method and in ISO 27005.

controller if they have little time to devote to the exercise (which is why it is recommended to place a copy of the risk illustration at the beginning of the document, in the management summary).

Among the many DPIA reports I have consulted, I have never seen a tree structure inspired by that proposed by ISO 13849-1:2023 (standard relating to machine safety), but I am not surprised by this absence. In the example (Fig. 1), the tree assigns a level based on the severity of the injury (S), the frequency and/or duration of exposure to the hazardous phenomenon (F) and the possibility of avoiding the hazardous phenomenon or limiting the damage (P).

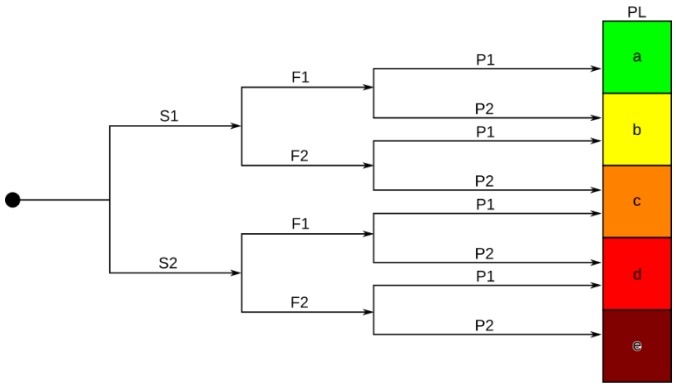

Figure1: ISO 13849-1 tree diagram

I also regret the underuse of the Ishikawa diagram (or cause-and-effect diagram), in the form of a fishbone, which accompanies a systematic approach to analysing a problem with multiple possible causes: we start with the result (the problem) – i.e. the head of the fish – and the bones are the causes or potential factors. It proves very useful in discussions about the measures to be taken to deal with a risk (e.g. in the event of a fire, firefighters start by cutting off the gas supply).

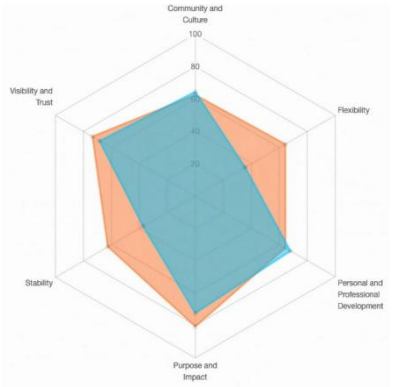

Figure2: Example of a Radar Chart (or Spider Chart)

On the other hand, I would have expected to see spider chart illustrations (or *Radar Charts,* see Fig. 2) in which each axis corresponds to a risk. The higher the level of risk, the further the point is from the centre. The points are then connected to form a surface. The smaller the surface area, the lower the exposure to risk.

This illustration allows both gross and net risks to be represented simultaneously (the effect of risk reduction measures can be seen at a glance) and allows an acceptability line to be added, but it does not allow the likelihood and severity assessments assigned to each feared event to be seen, as this information is provided in the text.

In this family of illustrations, there is a less common variant derived from the EBIOS Risk Manager method (Fig. 3). It was presented by Philippe Bost, DPO of Clermont-Auvergne-Métropole, during an experience-sharing session at the AFCDP in 2022. Here, the scale is reversed compared to Figure 2: the stakeholders most exposed to risk are those located near the centre. In this representation, the green border corresponds to the monitoring zone, the yellow border to the control zone and the red border to the danger zone.

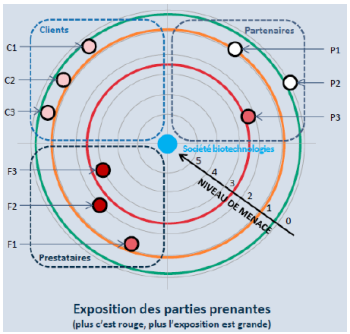

Figure3: Another example of the use of the Radar

Finally, it is worth noting the presence in the CNIL's PIA tool of a simplified Sankey diagram[9] , integrated to visually link potential impacts, threats, sources and measures to the three types of possible losses[10] (confidentiality, integrity, availability).

[9] Named in honour of Irish captain Matthew Henry Phineas Riall Sankey (1853-1926), who used this type of diagram as early as 1898 in a publication on the energy efficiency of a steam engine, although Frenchman Charles Joseph Minard had been using this type of graphic representation since 1869.

[10] Personally, I have never incorporated such a diagram, as I did not understand its value.

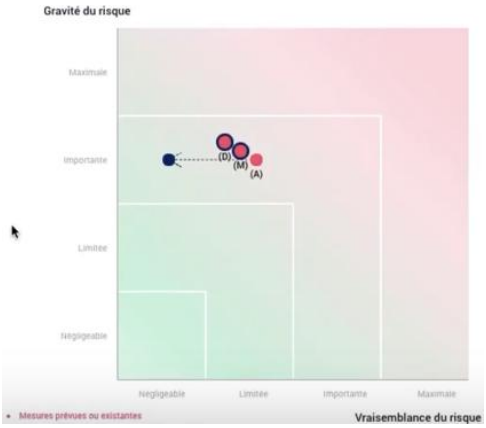

Figure 4: Extract from the video presentation of the CNIL's PIA tool (gross risks are in red, net/residual risks are in blue)

However, it is a matrix visualisation (also known as a *Risk Heat Map* in Anglo-Saxon literature) that seems to have become the norm within the DPO community. This practice actually originates from the world of risk analysis (rather than impact analysis), which explains why the CNIL includes one in several of its documents[11] (such as the one entitled "*Data protection impact assessment - Models*", on page 24) and in its PIA tool. The matrix generated by this tool presents a "risk likelihood" axis on the x-axis and a "risk severity" axis on the y-axis. These axes are ordinal and each has four levels, using a single set of terms. Only two colours are used, green and red, with a gradient.

What is the origin of the matrix?

The matrix has its historical origins in Farmer's diagram (Fig. 5), albeit with some adaptations. Frank Reginald Farmer (1914–2001) worked for the Safety and Reliability Directorate of the UK Atomic Energy Authority. In 1967, he proposed a representation to visualise the risks posed to society by a technology, project or activity (in this case, selecting the location of nuclear power plants taking into account the risk of iodine-131 leaks[12]). It is also known as an 'F-N diagram', in which the vertical scale (F) indicates the frequency of feared events, while the horizontal scale represents the consequences (usually the number of deaths, N). The left side of the curve shows frequent events that affect only a few people, while the right side represents rare incidents that cause large numbers of casualties.

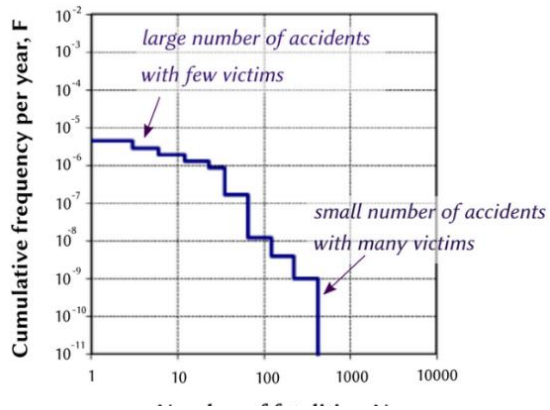

Figure 5: Farmer's diagram

This type of representation is often enhanced with tolerance limits: an upper line marks an "intolerable" zone above it, while a lower line marks a zone below it where the risks are considered negligible. The space between these two lines corresponds to the risks that are assumed, with treatment and monitoring. We will see later how this notion of "acceptability threshold" makes sense in the context of an impact assessment within the meaning of the GDPR (yet few matrices included in the DPIA contain it).

The first step is to familiarise yourself with the existing situation

Before tackling your first DPIA, the priority is to familiarise yourself with the organisation's practices and customs regarding risk management, and in particular to find out what representations are already used to represent them in other fields (such as customer, financial or operational risk assessment) and the scales used to qualify them in terms of likelihood and severity. If these approaches are appropriate for understanding impact assessments within the meaning of the GDPR, it may be difficult – or even counterproductive – to deviate from them, as management will be accustomed to the representations that have long been presented to them and will likely want a certain consistency in illustration styles (and scales) to enable comparisons. Conversely, if you are appointed as DPO within an organisation that has little

[11] The expert who, within the CNIL (after working at the ANSSI), laid the foundations for the Commission's doctrine on impact analysis, based his work on ISO27001 (he was also President of the EBIOS club).

[12] See the article "*Farmer's diagram, or F-N curve - Representing society's degree of catastrophe aversion*" by Eric Marsden, July 2022.

experience in risk management, you may be the one to set the tone by implementing your method, which could then be used to illustrate other types of risks facing any organisation.

The matrix is not "isolated"

The risk matrix is simply a visual representation of the method used to assess each feared event. It is therefore closely linked to the approach adopted[13] . Although this is not the subject of this article, it is not possible for me to properly discuss the visual representation (the matrix) without *at least* touching on the process that leads to it (moreover, the person who led the GDPR impact assessment must be able to answer one of the legitimate questions that a manager who is asked to endorse the residual risks may raise: "*But how on earth did you position this risk in this place in the matrix?*"). Therefore, even though this is not the subject I am addressing in this document, I feel compelled to offer a summary.

There are two main families of methods[14] : those based on calculation (known as "quantitative") and those based on human judgement (known as "qualitative"). The first category aims to be objective (neutral), as described in the paper entitled *Quantitative Privacy Risk Analysis*, published in 2021 by R. Jason Cronk and Stuart S. Shapiro. Probability is determined by a calculation that takes four factors into account: opportunity, motivation, capability and difficulty. Opportunity is expressed by the number of times (in a given period of time) that the risk factor is present. Motivation is a random variable that represents the probability that a threat actor will seize an opportunity. Ability is a random variable that represents the level of skills and resources that must be mobilised to carry out an attempt. Difficulty is a random variable that represents the level of obstacles that stand in the way of carrying out an attempt. The calculation is done in three steps: First, the frequency of attempts must be calculated, which is a function of opportunity and motivation and is calculated using the Monte Carlo method[15] . Then, again using a Monte Carlo simulation, vulnerability is calculated based on capability and difficulty (of execution), and finally, frequency is derived from the frequency of attempts and vulnerability (again, using a Monte Carlo simulation). Unfortunately, the document does not provide any concrete and easily understandable examples of how this method is applied. This approach requires loss data[16] , which is relatively rare. In this

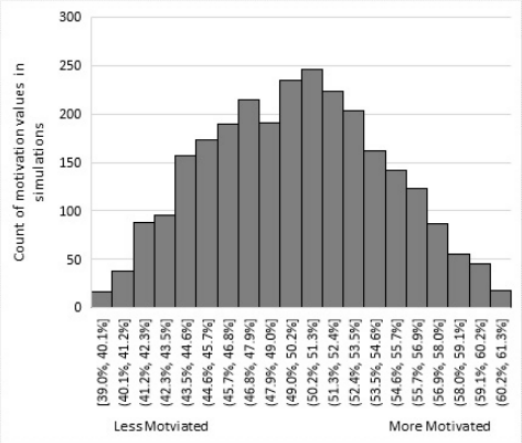

Figure 6: Histogram of simulation results for different possible motivation percentages

[13] Currently, the GDPR does not impose any particular method, as long as the eligibility criteria listed in the guidelines are met. The method chosen should be documented, "defensible", reproducible and verifiable, and produce a comprehensible deliverable. It is up to you to choose the method that you feel is most appropriate (the one promoted by the CNIL is not mandatory and in no way guarantees that you will produce a DPIA that the Commission will find fault with), bearing in mind that almost all existing methods were originally designed to address "risks to the organisation" rather than to the individuals concerned.

[14] In its document *Compendium of risk-management frameworks with potential interoperability*, ENISA describes around twenty risk analysis methods.

[15] Monte Carlo simulation is an algorithmic method for calculating an approximate numerical value using random processes, i.e. probabilistic techniques.

[16] In his document *Risikoanalyse und Datenschutz- Folgenabschätzung* (Risk Analysis and Data Protection Impact Assessment), the Bavarian Data Protection Commissioner gives priority to qualitative methods and is cautious about the use of accident statistics: "*The probability of occurrence can therefore be substantiated by existing circumstances, by one's own experience and that of others, as well as by statistics. With regard to statistics, however, the conditions under which they were compiled must be taken into account, as they were designed for a specific purpose and cannot therefore be transposed as such to the particular needs of the institution. Furthermore, the interpretation of statistical results is, in principle, a source of uncertainty.*"

case, the associated matrix has quantitative scales (rather than ordinal scales[17]). As part of Cyber Mondays, I followed with interest a presentation by the company Citalid on the method it has developed to assess the cost of a disaster in advance and decide whether to invest in countermeasures. Noting that there is a severe lack of data on cyber risk, they created a Bayesian model (using Monte Carlo simulations) which they calibrated with the limited data initially available and which they update as soon as new data becomes available. The results are therefore expected to improve as more data on incidents becomes available. The model takes into account the frequency of the threat, the probability of a disaster, the probability of suffering losses and the extent of those losses. This method, designed for "cybersecurity risks", is not applicable as such to DPIA in the context of the GDPR. Furthermore, as its authors have told me, it focuses on "frontline adversaries" and does not take into account internal sources of risk (poor design, poor software quality, human error, failure to follow instructions, etc.).

The second family (the "qualitative" one) is more subjective and is based primarily on the feelings of the stakeholders in the impact analysis (the MOA project manager, the MOE project manager, the RSSIs, the Risk Manager, the PRA/PCA-responsible " ," the subcontractor, the representative of the persons concerned... and, of course, the DPO). Drawing on their experience, more or less aware of incidents that have already occurred and influenced by their *preconceptions*, these actors assign likelihood and severity scores to each feared event. The current CNIL method is representative of this approach, which proposes ordinal scales each comprising four values (in this case, it is the writer and the evaluator who express their opinions on this subject).

Unsurprisingly, each formula has its advantages and disadvantages[18] , which is why the most commonly used methods today are "semi-qualitative" in the sense that they attempt to frame subjective assessments within a reassuring "scientific" framework. The ENISA method for assessing the severity of a data breach is a good example of this, with a superb equation that inspires confidence: SE = DPC x EI + CB, where DPC (*Data Processing Context*) is calculated based mainly on the type of data breached, its classification, the volume of data and its freshness, EI (*Ease of Identification*) corresponds to one of four levels relating to the "ease" with which an individual could be identified from the breached data[19] and CB (*Circumstances of the Breach*) to take into account the specific context[20] . This formula produces a result that is then positioned on a four-level ordinal scale (*Low*, *Medium*, *High* and *Very High*). Applied to the breach of Deezer customers' personal data, which earned its Israeli subcontractor *Mobius Solutions Ltd* a €1 million fine from the CNIL[21] , this formula gives a result of 3, i.e. *High*. If Deezer had taken the precaution of entrusting its service provider with only pseudonymised data (which was sufficient to perform the requested service), the result would have been only 1.5, i.e. *Low*. This is a way of objectively demonstrating to management the need to implement certain risk management measures. Nevertheless, it is clear that, depending on the values selected to perform the calculations (averages? medians? extremes?), the final result can vary considerably (as I have experienced in several real cases), which makes the rigour of the algorithm questionable. In its document "*Recommendations*

[17] *In mathematics, an ordinal number is an object that characterises the type of order of any well-ordered set, just as in linguistics, the words first, second, third, fourth, etc. are called ordinal adjectives and are used to specify the rank of an object in a collection or the order of an event in a sequence.* - Source: Wikipedia

[18] To my knowledge, there are no ideal methods for assessing risk that are free of flaws. The important thing is that they are used with a good understanding of their biases and limitations.

[19] This raises a question to which I have not (yet) found a satisfactory answer: Given the enormous amount of personal data that has been subject to data breaches (surname, first name, date and place of birth, social security number, email address, etc.) and published on the Darknet, can this information be considered "public" [this concept is never precisely defined], which would reduce the EI factor and the final risk level?

[20] Surprisingly, in its *PDB Assessment Methodology* document, the ICO uses another version of the same equation, in which the DPC and EI factors are added together (instead of multiplied): SE = DPC + EI + CB. The UK authority states that the method is not prescriptive "*and has been adapted from ENISA's recommendations for a methodology for assessing the severity of personal data breaches*" but does not explain the reason for this variation.

[21] See Deliberation SAN-2025-014 of 11 December 2025

for a methodology of the assessment of severity of personal data breaches", ENISA advises against placing blind trust in the "scientific" appearance of this approach: "*It should be remembered that both data controllers and competent authorities must exercise particular vigilance when dealing with cases which, due to their specific characteristics, cannot be properly assessed using this methodology.*"

Here is another example of a semi-qualitative method, suggested by the CNIL in 2012 (this approach has since been abandoned): It consisted of first considering the vulnerability of the media (from 1. "*Negligible - It does not seem possible to carry out the threat*" to 4. "*Maximum - It is extremely easy to carry out the threat*"), then estimating the capacity of the sources of threat to carry out their misdeeds (from 1. "*Negligible - They do not seem to have any capacity*" to 4. "*Maximum - They have unlimited capacity*"). The two results obtained were then added together. If the total obtained is less than 5, then the likelihood is negligible (1); if it is equal to 5, the likelihood is limited (2); if it is equal to 6, the likelihood is significant (3); and if the total is greater than 6, then the likelihood is maximum (4). The CNIL specified that "*This rating may be increased or decreased by other factors, such as openness to the Internet or a high degree of system heterogeneity.*"

The PRIAM [22] *method* uses both approaches, but in succession. For its authors, this combined approach avoids the biases of each approach: "*Probabilities can be calculated in different ways, either symbolically (based on a fixed scale of levels such as 'negligible', 'limited', 'significant', etc.), or using numerical values (probabilities). Each approach has advantages and disadvantages. As a general rule, probabilities can be difficult to estimate for input values and may seem difficult for decision-makers to grasp. Conversely, symbolic values are sometimes too vague and can lead to different interpretations.*"

The complete steps for computing likelihood are as follows:

1. Find the value of *exploitability* for each leaf node in the harm tree.
2. For each exploitation, choose the values of the relevant attributes of the risk source most likely to exploit the privacy weakness leading to the harm.
3. Find out the likelihood of each of these exploitations from the above *exploitability* value and values of the relevant risk source attributes.
4. Compute the likelihood of each feared event and harm according to the following rules[30], where P_i is the likelihood of ith child node:

Figure 7: PRIAM method for assessing likelihood

likelihoods of the child nodes.

R3. OR node with independent child nodes: $1 - \prod_i (1 - P_i)$.

R4. OR node with dependent child nodes[32]: $\sum_i P_i$.

To establish the likelihood of a risk, the PRIAM method begins by establishing "damage trees[23] ", starts by processing symbolic input values, converts them into numerical values so that they can be associated with the damage trees, and then transcribes them back into symbolic values for the final output. I am not aware of any AIPD that has been carried out using this method.

The best-known qualitative method is EBIOS Risk Manager, in which risks are identified and assessed during workshops[24] attended by stakeholders. Rédouane Djedir, DPO at Bred (Banque Populaire group), during his presentation entitled "*Help, I have too many PIAs to do!* " as part of the AFCDP's 2025 University for DPOs, explained that he participates in the workshop during which risks are identified and assessed (in terms of likelihood and severity) alongside representatives from the relevant business line, the IT department, the CISO and, where applicable, subcontractors. However, he deliberately keeps his distance from the workshop during which stakeholders identify the most appropriate treatment measures, in order to empower these actors.

[22] Sourya Joyee De, Daniel Le Métayer. *PRIAM: A Privacy Risk Analysis Methodology*. [Research Report] RR-8876, Inria - Research Centre Grenoble – Rhône-Alpes. 2016.

[23] The root of a tree represents damage. The leaves represent confidentiality weaknesses exploited by the most likely source of risk for the damage in question and are represented by pairs (confidentiality weakness, source of risk). The tree is structured into branches leading to the damage.

[24] The workshop method belongs to the SWIFT (*Structured What-If Technique*) family of analyses.

This method has many advantages, as it is based on human analysis. However, it generates a certain amount of work ([25] ly involving many people) and, above all, can suffer from a phenomenon of self-censorship (no one dares to speak or mention past incidents, some of which have not been brought to the attention of the DPO), or even produce biased consensus due to social conformity on the decisions of an individual within a group, as highlighted by psychologist Solomon Asch of the University of Pennsylvania in 1951 (In the experiment he conducted, a "naive" subject ended up declaring that a line, which was clearly shorter than the others, was not shorter, thus agreeing with the opinion of the other members of the group, who were accomplices instructed to give the wrong answer). For my part, I have adapted the Delphi method[26] (which I teach as part of my training course "*Conducting an Impact Assessment - From Theory to Practice*"), which allows us to avoid this pitfall and place less pressure on stakeholders. When using this approach, it is up to the DPO to counter biases[27] , such as recency bias, which leads to overestimating risks that have occurred recently (and, conversely, underestimating older ones).

Ultimately, however, it is the opinion of the data controller (who, according to the GDPR, "carries out" the DPIA) on the risks and their severity that prevails. When it comes to risks that affect others, some people do not take their reasoning very far. I am thinking, for example, of the statement made by the CEO of Voyageurs du Monde after 10,000 passports were stolen[28] : "*They're making a big deal out of nothing.../... These are only copies and no biometric data was collected by the hackers.../... Frankly, we're not worried*," or more recently, the statements made by the president of a departmental hunting federation in the Jura after a hacker put the data of 1,416,000 hunters up for sale on the *Dark Web*[29] : "*I'm not worried. I don't see what anyone could do with this information. It's not vital.*" When we know that, following the theft of data from members of the shooting federation, the cyberattack was followed by assaults and thefts of firearms from several members in several cities in France[30] ...

Be aware of the original "flaw"

Most of the methods developed in recent years to carry out impact assessments within the meaning of the GDPR are in fact adaptations of processes originally designed to conduct risk analyses. It is therefore important to bear in mind certain key differences between the two approaches in order to better understand the poor quality of most DPIA carried out using these methods and, above all, to take measures to address biases.

[25] Estimated at 7.5 hours per participant, not including the time required to organise the workshops, i.e. approximately 180 to 200 man-hours in total.

[26] The Delphi method was developed in the 1950s by Olaf Helmer and Norman Dalkey of the *Rand Corporation*. Its name refers to the Oracle of Delphi, a priestess at the temple of Apollo in ancient Greece, famous for her prophecies.

[27] Cognitive biases can alter judgement, influence decisions and increase the risk of error, such as confirmation bias or anchoring bias. Group bias occurs when a group makes decisions to maintain cohesion and avoid conflict, even if it means ignoring relevant options or adopting less than optimal solutions. Recency bias involves placing greater importance on the most recent information. In an impact assessment, this can lead to overestimating recent events at the expense of the bigger picture, which can result in inappropriate decisions.

[28] See "*My analysis of the cyberattack that affected Voyageurs du Monde*," Bruno Rasle, 8 June 2023

[29] See "*Hackers steal personal data: more than a million hunters could be affected*," by Emmanuel Deshayes, France 3 Bourgogne Franche-Comté, 22 January 2026

[30] Here too, applying the ENISA formula to assess the severity for the individuals concerned can lead to very different results depending on the input values selected.

To begin with, whereas an impact assessment focuses on the fate of the individuals concerned[31] , risk analysis focuses on the risks to the organisation[32] . In a way, a DPIA is an altruistic exercise, whereas risk analysis is a selfish approach. By carrying out a risk analysis, the organisation decides on its "risk-taking" for itself. The risk is therefore the coexistence of uncertainty (the potential consequences of the actions taken) and a challenge. When the organisation takes a risk for itself, it undertakes an action with the hope of gain and/or the possibility of loss. But by carrying out a DPIA, the organisation decides on the level of risk... that it will expose third parties to. The data controller is interested in the stakes (what it has to gain) but does not bear the uncertainty, which it imposes on the data subjects, most of the time without even informing them[33] or consulting them. Admittedly, Article 35.9 of the GDPR states that "*Where appropriate, the data controller shall seek the views of the data subjects or their representatives on the intended processing*", but this is rarely done. Yet who better than the data subjects themselves – the potential future victims – are best placed to assess the impact that the feared events could have on them[34] ? Could it be that there is a fear of their reaction when they read the risk matrix that has been drawn up?

Secondly, risk analysis methods focus on security risks, which are most often technical, and on attacks[35] . Thus, in the report "*Impact Analysis on Data Protection: the case of connected cars*" published in 2021 by the "Values and Policies of Personal Information" chair at the Institut Mines-Télécom[36] , I note the following passage: "[The CNIL method] *is nevertheless open to criticism on several points .../... by focusing solely on IT compliance.../... analysing the risks to personal data protection through IT security risks distorts the first category of analysis*." This is clearly evident, for example, in the document "*EBIOS Risk Manager - Another method of assessing likelihood*", in which all the criteria are based on the concepts of attacks and attackers[37] (for example, the criterion entitled *"Sense of impunity*", which defines the attacker's fear of being caught in the act). And in the booklet dedicated to the same method published by ANSSI, none of the examples listing sources of risk mention employees, application designers, developers or hardware incidents... even though many situations that are detrimental to the people concerned are caused by a failure to follow instructions or poor software quality, risks that are too often overlooked. As the organisation has failed to list this type of feared event, the DPIA will be of poor quality as no risk treatment measures will be put in place. I remember a case where, because of one of our processing operations, a data subject found themselves banned from banking. As the origin of the risk was not security-related, this risk had not been identified and remained unaddressed. In such a situation, it is up to the DPO to contact the person responsible for drafting the acceptance criteria in order to detect design flaws. In another case, the feared event was caused by insufficient information provided to individuals (the measure taken was therefore to improve this information). Here again, methods derived from risk analysis too often overlook this type of issue. It is therefore crucial that DPOs do not "abandon" the

---

[31] And it cannot be repeated often enough that the risks that must be taken into account are all those that could impact the rights and freedoms of individuals in relation to the processing of their personal data. The WP248 guidelines emphasise this point: "*The reference to the rights and freedoms of data subjects refers primarily to data protection and privacy rights, but also includes, where applicable, other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, the right to liberty, and freedom of conscience and religion*." I am therefore surprised to hear that the RFIA to be carried out as part of the RIA will *finally* take all rights and freedoms into account. Is this not a sign that AIPDs are often carried out half-heartedly?

[32] The impact of a feared event on customers is only considered through the prism of its impact on the company (loss of market share, decline in average basket size, etc.).

[33] Risk-taking is then described as involuntary.

[34] In his "*Traité de riscologie*" (Imestra Editions, 2009), Georges Jousse discusses the factor of sentimentality, which means that the value of the consequence of a feared event is not the same depending on whether or not the person assessing it feels concerned by the risk.

[35] "*The main objective of risk management is to protect information systems (software, hardware, systems, components, services) and business assets, and to minimise costs in the event of failure*," ENISA, *Risk Management Standards - Analysis of standardisation requirements in support of cybersecurity Policy*, March 2022

[36] This document contains a very interesting comparison between four methodologies (those of the CNIL, PRIAM, BSI and NIST) and recommends studying the LINDDUN method (for "*Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance*") proposed by researchers at the Belgian university Katholieke Universiteit Leuven. This method makes it possible to identify threats during the development of IT projects.

[37] The method focuses on "intentional and targeted threats". And, according to Club EBIOS, "*the aim is not to identify all risks, but only the most significant ones*".

implementation of DPIA to CISOs and IT specialists alone and ensure that their thinking extends well beyond security and technical risks (for example, ensuring that there is no misuse of data).

Thirdly, risk analysis methods often only consider three types of incident: loss of confidentiality, loss of integrity and loss of availability. While it is indeed necessary to start there, it is important to take the discussion further, as there are feared events that do not belong to any of these categories[38] . I remember a project in which the individuals concerned would have been unable to apply for social benefits, even though none of the three losses mentioned *above* would have been observed. Another example is the risk that the treatment could generate a *chilling effect* – the fact that the persons concerned feel prevented from exercising a right, tend to self-censor or refrain from carrying out an activity for fear of the repercussions (pressure, reprisals, prejudice) they might suffer.

Finally, since the entity at the centre of a risk analysis is unique (the organisation conducting it), it is easy to quickly compile a list of feared events whose consequences are fairly easy to assess. In this case, a single risk matrix is sufficient. Conversely, in the context of a GDPR impact assessment, the same processing may concern individuals who will be exposed to very different risks. When each feared event occurs, some will suffer no inconvenience, while others will suffer catastrophic consequences. Does it therefore make sense to produce a single risk matrix? Would it not be better to produce a risk matrix for each homogeneous population[39] and even go so far as to study specific risk treatment measures for each population? Some risk assessment methods use the concept *of a utility unit,* which serves as a unit of value to attempt to assess the impact on each person concerned. For example, following a coach accident in which several passengers suffered a severed finger, the same event would be estimated at a low number of utility units for a footballer... and a much higher number for a violinist. As Georges Jousse points out in his "*Traité de riscologie*" (Treatise on Riskology), it is rare for the nature of the consequence to be the same for all victims. It is therefore quite conceivable to produce an AIPD comprising several matrices, each dedicated to a homogeneous population. Logically, the processing measures would be differentiated (rather than global), in order to provide greater protection to the persons concerned for whom the impact will be greatest. Thus, it is not uncommon for the consultation of the files of "VIP clients" (politicians, celebrities, etc.) to be subject to enhanced control. We can also think of entities authorised to process data that, when read, reveal the military status of certain data subjects.

What are the most common matrices in France?

[38] This is stated by the EDPS in its document *Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation*, July 2019: " *Although there is a close link with information security risk management (as it is not possible to ensure good data protection without good data security), the risks to be taken into account in a DPIA go beyond those affecting the traditional objectives of an IT risk analysis, namely confidentiality, integrity and availability.*"

[39] This seems to be the recommendation of the Office of the Privacy Commissioner of Canada in its guide to the privacy impact assessment process: "*You should consider the impact your initiative may have on the privacy rights of different groups. For example, you could conduct a gender-based analysis to determine the potential impact of policies, programmes and initiatives on various groups of women, men and non-binary persons from a privacy perspective.*"

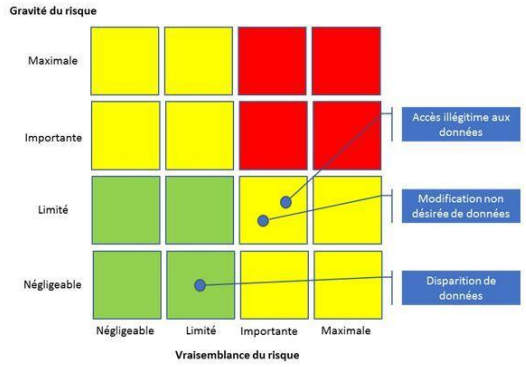

Figure 8: Risk matrix frequently observed within DPOs (France)

No doubt due to the CNIL's PIA tool (and its inclusion in many tools on the market designed to help organisations comply with the GDPR), a de facto standard seems to have emerged within the French DPO community: a 4 x 4 matrix, with the "*likelihood of risk*" axis on the x-axis and the "*severity of risk*" axis on the y-axis. Among DPOs who no longer generate the matrix using the CNIL tool, the most frequently observed colours are green, yellow and red, with the distribution shown in Figure 8.

The debate over the number of rows and columns is endless among risk management experts[40] . For proponents of the first approach, an even number avoids positioning everything in the median values and forces the respondent to make a choice. With its odd number format, it is true that stakeholders are often tempted to opt for a median opinion (the "lukewarm" effect). This risk is particularly high in matrices with only a small number of rows and columns. This should be considered a potential bias: the neutral option can be a safe choice and attract the majority of responses. In this case, the assessments may not be meaningful and the relevance of the AIPD may be called into question.

Naturally, a higher number of rows and columns provides more nuanced data and minimises the bias mentioned *above*: this is why I find 3x3 matrices (used, for example, by the ICO - *Information Commissioner's Office*) to be of little relevance.

It is also necessary to determine the type of scales used on both axes (and if they are imposed on you by a tool, to understand their nature). They can be ordinal or quantitative, depending on the method used to assess the risks. In an ordinal scale (most commonly used in AIPDs), risks are ranked (in order). The number associated with each rank (or level) indicates only a rank and not a quantity. Thus, a risk ranked in the fourth row is not twice as "great" as another risk ranked in the second row. This type of scale only indicates that the first risk is greater than the second (it is used solely to assess the severity of risks in relation to each other). There is therefore no consistency or regular progression between levels[41] . Care must therefore be taken with the value of the differences between each rank, as otherwise this type of scale can lead to erroneous conclusions. The following example[42] leaves me sceptical. It is based on scales of four values. The severity scale includes the levels "*Limited = Almost no impact*", "*Significant = Minor impact*", "*Critical = Significant consequence(s)*" and "*Catastrophic = [Up to and including] Danger of death*". Personally, I find the differences between these four values to be uneven, with a particularly wide gap between "*Significant*" and "*Critical*". Furthermore, I find the term "*Significant*" to be somewhat unrelated to the proposed definition ("*Minor impact*"). It would probably have been better to opt for a five-point scale (allowing for greater nuance and a more gradual progression between levels) and to choose the terms (and definitions) associated with each level more carefully.

[40] See, for example, the following passage from the document "Le supplément" associated with the EBIOS method (Anssi) on page 14: "*The use of a 4- or 5-level scale is guided by the following considerations: the need to measure very high impacts corresponding to major crises, or even destabilisation and loss of resilience beyond the organisation concerned. In this case, a 5-level scale is recommended. Otherwise, 4 levels will suffice*." Note that the MIL-STD-882B standard uses a 4x5 matrix (*Severity x Probability*).

[41] The following paper discusses other possible biases: *Problems with Risk Matrices Using Ordinal Scales*, Michael Krisper, Institute of Technical Informatics Graz University of Technology (Austria), March 2021

[42] Example found on the website macartodesrisques.fr, a free platform dedicated to SMEs and mid-cap companies, developed by Amrae and Medef Deux-Sèvres, which allows users to perform a self-assessment and risk mapping (for companies) in just a few clicks.

In a quantitative scale, each risk is assigned a number between 0 ("*This will definitely not happen*", for example, concerning likelihood) and 1 ("*This will definitely happen*") on each axis, with all intermediate values possible. Some go so far as to consider completely removing the human element from this type of approach, such as Luis Enríquez, who spoke about the use of the FAIR model[43] on AI-related risks at the FAIR 2023 conference: "*I believe that DPOs and CISOs are neither judges nor administrative authorities, and that they do not have the necessary training and skills to predict the impact on the rights and freedoms of individuals. So how can they assess the impact of data processing on data subjects? To build my Pd-VaR (Personal Data Value at Risk) solution,[44] , I used scientific study of the legal system and predictive data protection analysis to implement research models based on historical data from published administrative sanctions. This helped me establish the profile of regulators' "sanction psychology" and obtain data from their legal reasoning. I then merged this data with the current state of risk-based compliance maturity of a data controller. My initial implementations were based on the FAIR model, but I was forced to adapt it to the GDPR.*

The importance of semantics

The likelihood axis of the representation proposed by the CNIL's PIA tool includes the following values: negligible, limited, significant and maximum. The same semantics are used to describe the levels of severity. I must admit that this similarity bothers me[45] . It seems to me that using terms more suited to each component of the risk would be more relevant. Take, for example, the semantics used in one of the examples provided by the EDPS in Figure 12 of its document *Report on DPIA survey 2024 to EU institutions, bodies, offices and agencies*. Here, each axis has five levels. For likelihood, the values are "*Rare*", "*Unlikely*", "*Possible*", "*Likely*" and "*Almost certain*". For severity, the scales are "*Very low*", "*Low*", "*Medium*", "*High*" and "*Very high*". In another document, the CNIL mentions a much more appropriate set of terms: "*Unlikely*", "*Occasional*", "*Common*", "*Very common*" (for likelihood) and "*Painless*", "*Limited*", "*Serious*" and "*Dramatic*" (for severity). By way of comparison, I would point out the terms used in the rating matrix of the standard that gave rise to the FMEA method with regard to severity ([46]): "*Minor*", "*Marginal*", "*Critical*" and "*Catastrophic*". It is clear that the choice of expressions can have an effect on the reader of the AIPD, who will undoubtedly react more strongly to a risk rated "Catastrophic[47] " than to one rated "*Maximal*".

We can take this reasoning further and seek greater ownership by the parties involved in the AIPD (and better understanding by the data controller) by using semantics that are even closer to spoken language, as seen in the Kinney-Wiruth method[48] , whose likelihood scale has seven levels: "*Virtually impossible*[49] ", *"Practically impossible*", "*Conceivable, but highly improbable*", "*Just possible*", "*Unusual but possible*", "*Quite possible*" and "*To be expected, certain*". Finally, if the chosen method takes into account a third axis, that of "detectability" (or "maturity"), its semantics must also be carefully determined. Thus, in this example, the following values are proposed (from best to worst): "*Proactive control (alerts)*", "*Controls in place*", "*Regular controls*" and "*No controls*".

---

[43] *Factor Analysis of Information Risk*

[44] See the paper *A Personal Data Value at Risk (Pd-VaR) approach*, by Luis Enríquez, 5 November 2024

[45] It is also found in ISO 29134 (Guidelines for privacy impact assessments), which uses the following terms (identical for both axes): Negligible, Limited, Significant, Maximum.

[46] See also the semantics noted in the document *Privacy Impact Assessment toolkit for Health and social care* by *the* Irish *Health Information and Quality Authority* (October 2017): negligible, minor, moderate, major and critical.

[47] *This is the term proposed in the document "Le supplément" (The Supplement) made available by ANSSI concerning the EBIOS-RM method to describe the highest level on the severity scale (see page 15).*

[48] *KINNEY G. F. and WIRUTH A. D. (1976) Practical Risk Analysis for Safety Management, NWC Technical publication 5865, Naval Weapons Center, China Lake, CA*

[49] This level (which is very rare) can be used to classify risks such as the 11 September 2001 attacks, the Fukushima tsunami, the blockage of the Suez Canal and the COVID-19 pandemic. In his essay "*The Black Swan: The Power of the Unpredictable*", statistician Nassim Taleb develops a theory according to which a black swan is a certain unpredictable event that has a very low probability of occurring and which, if it does occur, has consequences of considerable and exceptional significance.

The question of defining rating scales

Beyond the attention that must be paid to the semantics used, each value on the rating scales must also be objectified[50] . Among the many AIPDs I have had the opportunity to read, unfortunately, there are few objective definitions, which gives the impression that this step has been overlooked. In most cases, the approach embedded in the method used has been adopted without really understanding or mastering it. However, some methods require careful consideration, such as EBIOS RM, which allows users to define their own method of assessing likelihood (although it focuses mainly on the reality of the attacker's success). Thus, for the CNIL, in the event of maximum severity, "*the individuals concerned could experience significant, even irreparable consequences that they may not be able to overcome*" - and the Commission cites the death of individuals concerned among a few examples, as does ISO 29134: "*Maximum - Data whose unauthorised disclosure, modification, loss or destruction could affect the existence or health, freedom and life of the individuals concerned. Individuals could experience significant, even irreversible, inconvenience and insurmountable consequences.*"

Allow me to return to the example I found on the macartodesrisques.fr website, which lists the levels of the likelihood assessment scale: "*Unlikely = This has never happened and there is no chance of it happening*"; "*Rare = This has never happened and is unlikely to happen*"; "*Occasional = It has happened a few times and is likely to happen again*"; "*Frequent = It happens regularly and will continue to happen* regularly[51] ". This scale is based on observed past events (i.e. known loss frequency), which is rarely the case. And what is the scope? Only the organisation carrying out the DPIA, or a broader scope, taking into account what has happened within other data controllers[52] ? Furthermore, the use of "*and*" implies that things are immutable: if the event has rarely occurred in the past, *then* it will automatically be the same in the future. Is this really the case? Shouldn't these "*and*" be replaced by "*and/or*" to encompass more realistic assessments?

In fact, it suffices to question several of the parties involved in the exercise to gather very different assessments for each level (not to mention the opinion of the data controller, who must assume the residual risks). Thus, in the audit report on DPIA carried out by the DPOs of European bodies in 2024 and published by the EDPS, the following criticisms are made: "*Some of the impact assessments audited do not specify how they arrive at a specific score rather than another... the criteria for assigning values to severity, probability and impact often remain unclear.*" "*Many of these DPIA do not provide any clarification on how they arrive at a specific numerical score. This is regrettable. We need to go beyond simply ticking boxes and ensure that numerical scores are assigned in a reasoned manner.*" The previous audit report (from 2020) already contained the following advice: *"To conduct your impact assessment, you are free to choose one of the existing methodologies or create your own, but for it to be fully effective, it must at least include: .../... a method for estimating the probability and impact of these events; a method for calculating the risks to data subjects based on the events, their probability and their impact.*" In his paper entitled *Review of the strengths and weaknesses of risk matrices*, Mustafa Elmontsri makes a similar criticism: "*The positioning of risks on the matrix is subject to numerous considerations, some of which may even escape the assessor. However, and this is a serious problem, the required explanations and justifications are rarely, if ever, provided.*"

It is true that objectifying the rating scales used is a difficult exercise that generates much debate. One example is the objectification of each "bar" on a severity rating scale: should the number of people potentially affected by the feared event be considered a relevant criterion? For example, a document from

[50] It is recommended that each definition be illustrated with a few examples. Thus, with regard to severity, we can imagine illustrating the first level with the receipt of unsolicited advertising (i.e. spam) and the "*High*" level with a banking ban or identity theft. For the last level ("*Very high*" or even "*Dramatic*"), we could mention divorce, suicide or severe disability.

[51] The definitions of each level should seek to clarify the corresponding frequencies. In these examples, what do "*a few times*" and "*regularly*" mean?

[52] In one of the examples of risk analysis (not impact analysis) published by Club EBIOS, the definition of the highest level of likelihood ("*4. Certain or already occurred*") answers this question: "*Such a scenario has already occurred within Club EBIOS or other similar associations*" (see page 17).

Monash University (Australia) includes "*small number of people affected*" among the criteria for determining minor impact. Similarly, the PRAM (*Privacy Risk Assessment for Data Subject Aware Threat Modelling*) method takes into account the number of potential victims to determine the severity of a risk. In my opinion, even if only one person were affected, the assessment of the impact of the risk should not take this factor into account in the context of a DPIA. For a victim, the fact that they are the only one suffering the consequences of the processing of personal data (or that they are suffering alongside others) is of little importance.

Which colours to choose?

Colours evoke emotions based on shared experiences that are deeply rooted in each culture. While in China red is the colour of luck and prosperity, in the West it evokes intense emotions such as passion, anger and danger, probably because it is the colour of blood. *Conversely*, the colour green conveys a sense of serenity as it reminds us of nature (and gives us freedom of movement). Thus, even without us realising it, colours can change our perception of things and can be used to influence our decisions. This is why we must choose carefully which colours to include in a risk matrix, as they will inevitably have an influence. We must also ensure that they correspond appropriately to the semantics mentioned *above*: it would be surprising to use the colour pink for a risk assessed as catastrophic!

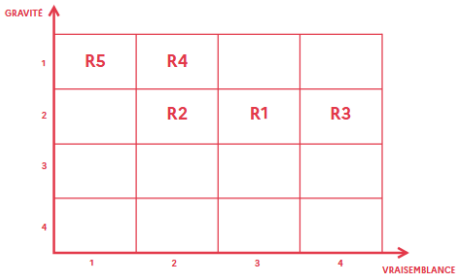

Figure 9: Example: "Biotechnology company supplying vaccines" - ANSSI

To begin with, I will set aside matrices that do not use colours at all – which are quite rare – such as the one featured in the video presentation of the CNIL's PIA tool or the one on page 72 of the ANSSI document "EBIOS Risk Manager – The Guide" (Fig. 9). Why deprive ourselves of the symbolic power of colours to make the data controller more aware of the issues associated with the processing project?

It is rare to find matrices that use only shades of the same colour. *At a minimum*, I have seen illustrations using three colours, as is often the case with the ICO (in a 3x3 matrix, Fig. 10) or the NIST (within a 5x5 matrix, taken from the document *Prioritising Cybersecurity Risk for Enterprise Risk Management* - NIST Interagency Report NIST IR 8286B-upd1 February 2025. Fig. 11).

Severity of impact				
	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Figure 10: Typical matrix used by the ICO

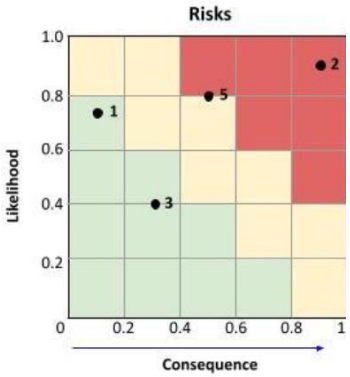

Figure 11: Typical matrix used by NIST

Although these two examples use the same colour palette (red for unacceptable risks, pink for controlled risks and green for risks that are only monitored), I note a feature that I find somewhat irrelevant in the ICO model, namely the fact that several green boxes are adjacent to red boxes. How can one move so quickly from one extreme situation to another? The NIST model avoids this violation of one of the rules

that should apply (two "extreme" boxes should never touch but should be separated by *at least* one intermediate colour[53]).

We then see matrices that use a greater number of colours, five for example in the model used in Singapore[54] (Fig. 12). The maximum I have seen in the GDPR impact assessments I have had the opportunity to consult is seven. It seems to me that we should not go beyond four or five colours, but I have not found any relevant studies on this subject.

IMPACT						
	Very Severe (5)	Medium (5)	Medium High (10)	High (15)	Very High (20)	Very High (25)
	Severe (4)	Low (4)	Medium (8)	Medium High (12)	High (16)	Very High (20)
	Moderate (3)	Low (3)	Medium (6)	Medium (9)	Medium High (12)	High (15)
	Minor (2)	Low (2)	Low (4)	Medium (6)	Medium (8)	Medium High (10)
	Negligible (1)	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)
		Rare (1)	**Unlikely (2)**	**Possible (3)**	**Likely (4)**	**Highly Likely (5)**
				LIKELIHOOD		

Figure 12: Model from the Cyber Security Agency of Singapore (CSA)

Although I myself used it in my first DPIA, I admit that I have stopped using the colour green in a GDPR risk matrix[55] because, culturally, it conveys the message that there is no risk... which is not true[56] . Furthermore, the area usually coloured in this way (generally the square at the bottom left, with low likelihood and severity ratings) is often accompanied by the following comment: "*No action required*".

For my part, I believe that implementing a detectability measure is, *at the very least*, essential, if only to verify the relevance of the assessments (Are these risks as rare as expected?) and to be able to revise the assessment if necessary. I note that, in his document *Risikoanalyse und Datenschutz-Folgenabschätzung*, the Bavarian Data Protection Commissioner presents a 4x4 risk matrix (Fig. 13) showing three levels of risk, coloured green, yellow and red. The accompanying text clearly states the existence of risks for the green zone: *"In terms of data protection, the risk index has exactly three levels. The GDPR uses the terms 'risk' and 'high risk', with the term 'risk' also being referred to as 'normal risk'. In addition, the GDPR mainly uses the phrase 'should not present a risk' " (Art. 27(2)(a) and Art. 33(1) of the GDPR). Given that there can be no completely risk-free processing, the expression "should not present a risk" is mainly understood, in view of its meaning and purpose, as "presenting only a low risk".*

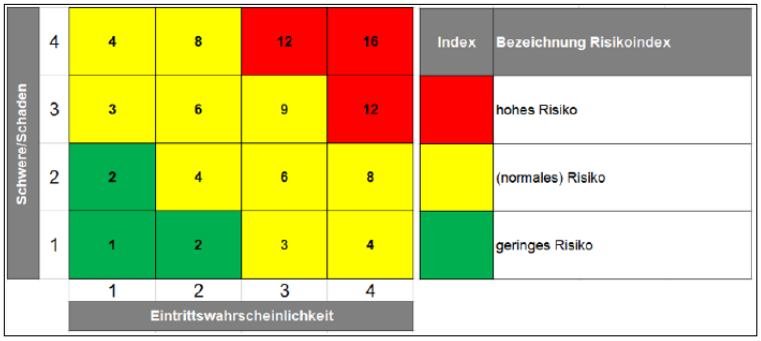

Figure 43: Matrix recommended by the Bavarian authority

[53] This is one of the rules outlined in the article *What's wrong with risk matrices?* by Louis Anthony Cox Jr (published in April 2008 in the journal *Risk Analysis*).

[54] See *Guide to conducting cybersecurity risk assessment for critical information infrastructure*, *Cyber Security Agency of Singapore* (CSA), 2019.

[55] On the other hand, I understand that the colour green is used in risk analysis (for the company) to indicate risks that management does not consider to be a priority.

[56] Surprisingly, in its *PDB Assessment Methodology* document, the ICO does not see the need to involve the DPO for risks in this area!

I was also surprised to see matrices or scales using colour gradients, as in the CNIL's PIA tool, even though the scales used are ordinal. As it is not possible to position the cursor on an intermediate value, I admit that I did not understand the logic behind this type of representation.

Figure 14: Extract from the video presentation of the CNIL's PIA tool

Representing an acceptability limit?

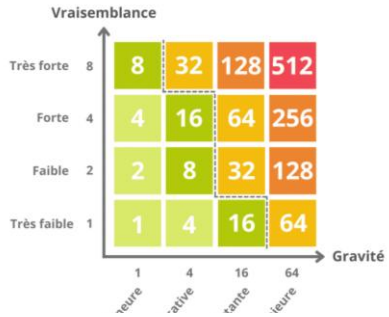

Figure 15: One acceptability limit, two zones

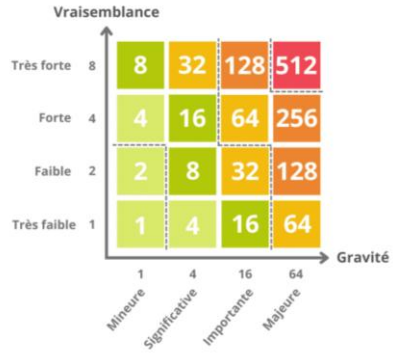

Figure 16: Three acceptability limits, four zones

The acceptability limit is one of the most important concepts in risk management. It is generally represented by a curve or a line, and divides the matrix into a maximum of three distinct areas: unacceptable risks, accepted and managed risks, and accepted but monitored risks.

Figure 15 shows an example with two areas[57] . Note that the entire line corresponding to major severity is positioned in the unacceptable risk area, even for risks with very low likelihood (note: the axes are reversed here compared to the most common representation).

And here (Fig. 16) is the same matrix showing four zones: the red box is positioned in the "unacceptable" zone (the prohibited area). If a net (residual) risk is found there, this should require the data controller to consult the CNIL under Article 36 of the GDPR[58] . Unfortunately, the source document does not indicate the decisions associated with the other zones. It is reasonable to assume that net risks in the first intermediate zone will need to be addressed and monitored very rigorously before processing is implemented, while those in the second intermediate zone will need to be addressed and monitored. Finally, those in the last zone (here, boxes 1 and 2) would only need to be monitored?

We can therefore clearly see the crucial consequences of setting acceptability limits for the data controller (and the project in question) – and the decisions associated with each zone. Depending on the positioning of residual risks and acceptability limits, the organisation may lose complete control of the timetable and become dependent on the supervisory authority (which may even refuse to allow the processing to be carried out) under Article 36 of the GDPR.

For my part, I regret that only a minority of DPIA contain a clear and explicit definition of these limits (which should be determined by the data controller and not vary from one impact assessment to another): I very rarely see them included in the matrices, even though they address the crucial issue ("*Does the overall level of residual risk require us to consult the CNIL?*").

[57] Source: https://pyx4.com/blog/comment-construire-echelles-de-cotation-des-risques/

[58] The attitudes of data controllers can vary, ranging from those who want to have as little to do with the CNIL as possible to those who want to cover themselves by systematically seeking its assistance. The balance tips towards the former.

An example of this can be found (Fig. 17) in one of the practical fact sheets dedicated to the GDPR and published by Clusif (French Information Security Club). In chapter 7 of the PIA fact sheet, we find the following passage: "*A residual risk can be considered high and unacceptable if it exposes individuals to significant or even irreversible consequences that they may not be able to overcome (e.g. unauthorised access to their data that could threaten their lives, lead to dismissal, or jeopardise their financial situation) and/or when it seems obvious that the risk will materialise (e.g. where it is not possible to reduce the number of people accessing the data due to the way it is shared, used or distributed, or where there is a well-known uncorrected vulnerability).*"

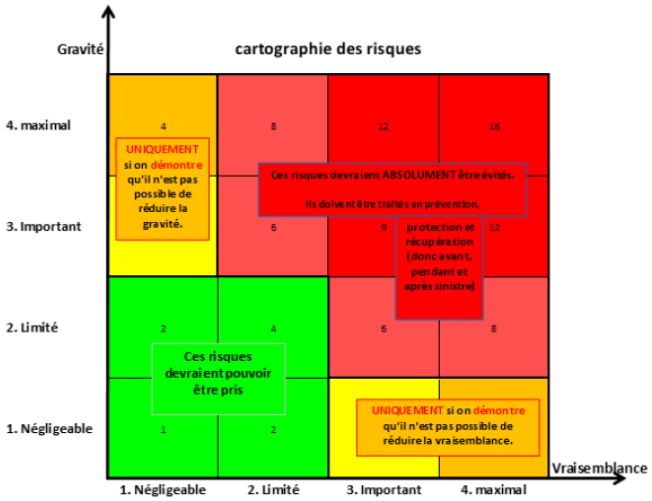

Figure 17: Example of a matrix clearly showing the rules that "trigger" Article 36. GDPR

The illustration is accompanied by the following comment: "*In cases where the severity is high and the likelihood is negligible, and in cases where the severity is negligible and the likelihood is high (i.e. for the two orange squares in the diagram), the organisation must seriously consider consulting the CNIL.*"

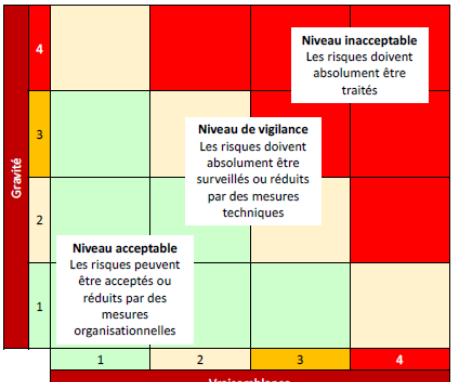

Figure 18: Decision matrix used by Club EBIOS

Another example can be found in one of the risk (not impact) assessment examples published by Club EBIOS (Fig. 18). It is worth noting the enormous differences between the two matrices (the Clusif and Club EBIOS matrices): although both are 4x4 matrices, the choice of colours and their distribution are completely different. Food for thought...

Below is a third example, produced by the AFCDP's "Health Data" group. The decision matrix (Fig. 19) is accompanied by the following definitions: "*Red: These risks should be avoided or reduced by applying security measures that reduce their severity and likelihood. Ideally, it would even be advisable to ensure that they are addressed through independent measures of prevention (actions before the disaster), protection (actions during the disaster) and recovery (actions after the disaster). Orange: These risks should be avoided or reduced by applying security measures that reduce their severity or likelihood. Prevention measures should be prioritised. They may be taken, but only if it is demonstrated that it is not possible to reduce their severity and if their likelihood is negligible. Yellow: These risks should be reduced by applying security measures that reduce their likelihood. Recovery measures should be prioritised. They may be taken, but only if it is demonstrated that it is not possible to reduce their likelihood and if their severity is negligible. Green: These risks should be taken, especially since the treatment of other risks should also contribute to their treatment.*

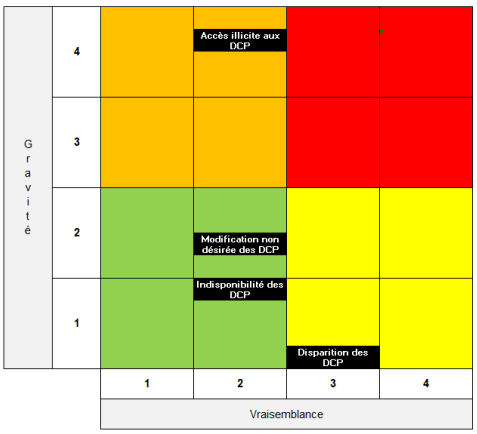

Figure 19: Decision matrix of the AFCDP's "Health Data" group

In this specific example, I shared three thoughts with the fellow DPO who led the work: 1) As I indicated *above*, I have a different opinion regarding the use of the colour green and the "non-decisions" associated with it; 2) I remain sceptical about the use of the colour yellow for all the boxes in the top row, since this same DPIA specifies that this level corresponds to *irremediable* risks (i.e. potentially the death of data subjects). With the objectified definitions, should the data controller not have been advised to consult the CNIL under Article 36 of the GDPR (whereas this matrix allows them to "fly under the radar" ... while exposing the data subjects to dramatic risks)? Finally, I also question the assessment of the severity of the unavailability of health data (here assessed at 2 in gross terms, i.e. "*It seems difficult for the identified sources of risk to realise the* threat[59] ") when compared to the death that occurred in a British hospital following a cyberattack that delayed the receipt of test results and caused delays in treatment. The patient died because his transplant was cancelled. It should be noted that in 2024, CERT Santé reported around 60 cases in France in which patients were put at risk due to security incidents.

The fact remains that several fellow DPOs (both internal and external) have admitted to me that they pitifully define the colours of the matrix and the limits of acceptability after positioning the residual risks, in order to satisfy their data controller (or their client) and avoid consulting the CNIL under Article 36 of the GDPR[60] . Not only does this reflect poorly on the quality of the DPIA produced, but it also creates time bombs that could cause problems for their authors if the authority becomes aware of them, for example during an inspection.

Does the matrix really enable measures to be prioritised?

Very often, in the literature on risk management, it is stated that the matrix would enable "*actions to be prioritised according to the level of severity identified for each risk*". While this statement makes sense in the context of a risk analysis – those weighing on an organisation, which makes a conscious decision to accept the threats it faces and can spread the implementation of treatment measures over time – it makes no sense, in my opinion, in the context of a GDPR impact assessment, if only because the measures must be implemented *before* the treatment is carried out[61] . And when it comes to the effective allocation of resources to deal with threats, the Ishikawa diagram[62] (fishbone diagram) provides better opportunities to identify where efforts should be focused.

The statement also makes little sense when we see matrices that use the same colour for boxes where the multiplication of likelihood and severity assessments gives the same result according to the frequently used formula $R_{(Risk)} = L_{(Likelihood)} \times S_{(Severity)}$. In fact, risk assessment is not linear in relation to each of the two variables, and this concept must be used with caution, as everyone understands that a feared event with a likelihood of 5 and a severity of 1 should not be perceived in the same way as an event with a likelihood of 1 and a severity of 5. Common sense dictates that we should focus our efforts on the second case (in which the treatment may cause the death of a person concerned) rather than the first (which will only result in

[59] Here we see the danger of limiting the assessment of likelihood to a single factor, in this case the "ease" with which the source of risk will materialise the incident.

[60] An extreme case is when the data controller commits forgery by modifying the opinion given by their DPO (which changes from negative to very positive) without the latter's knowledge. See *Il faut sauver le soldat DPO !* (We must *save the DPO*!), page 17, Bruno Rasle, 5 May 2023

[61] In some cases, however, additional measures may be deployed after the processing has been implemented, provided that they are not necessary to reduce a risk to a clearly acceptable level. For example: it was decided to reduce the retention period for processed personal data in order to reduce exposure to risks. When formalising the DPIA, it was decided to implement an automatic purge in order to lighten the load. Due to a lack of time (and/or budget), this measure could not be deployed. The processing was therefore implemented with a manual and supervised purge. The DPIA, which was submitted to the data controller for signature, includes a commitment to enhance the processing of this automatic purge function from the next financial year onwards.

[62] The cause and effect diagram, or Ishikawa diagram, or fishbone diagram, is a tool developed by Japanese engineer Kaoru Ishikawa in 1962 and used in particular in quality management.

nuisance for those affected). This observation should encourage us to use a more "alarming" colour for all boxes corresponding to maximum severity.

If, in the context of a PIA, traditional matrices do not help us prioritise the implementation of risk treatment measures (avoidance or impact reduction), they can nevertheless be useful for identifying risks that require increased supervision (in other words, those that need to be monitored "*like milk on the stove*"). In this case, if we return to the example mentioned *above*, it would be prudent to set up alerts and carry out regular checks in order to be able to detect the occurrence of feared V1/G5 events as quickly as possible. It would be illogical not to have a function for detecting events[63] . In my teaching, I recommend that, for each feared event, the following question be formally considered: "*Are we/would we be able to detect its occurrence?*" If the answer is no, the action plan submitted for signature by the data controller must include the implementation of traceability (as the CNIL frequently points out in its deliberations[64]) and an effective procedure for exploiting it, including synchronously (and not just *post-mortem*[65]). As a precautionary measure , regular checks should be carried out to ensure that detectability remains operational, so as not to find oneself in the situation of Free Mobile, whose defence, when it appeared before the CNIL's restricted panel on 15 December 2025, indicated that its client was indeed equipped with a system for detecting malicious behaviour, but that this had been neutralised during an upgrade. There are also risk management methods that incorporate this dimension of detectability in addition to that of likelihood and severity (an undetectable event receiving a high score, which increases the level of risk calculated according to the formula R(Risk) = L(Likelihood) x S(Severity) x D(Detectability)), The best known of these is the FMEA (Failure Mode, Effects and Criticality Analysis) method, developed by the US military in the 1940s.

Let's try to formulate some advice...

Through my research, discussions with my peers and reflections, I have come up with some advice for my fellow DPOs:

1. **You shall assume your role as methodological guarantor:** In its guidelines on DPOs[66] , the G29 recommends that the data controller seek advice from their data protection officer, particularly on the methodology to be followed when carrying out a data protection impact assessment. In addition to verifying that the result produced meets the requirements listed in Annex 2 of the guidelines on DPIA, you must select a method that is capable of providing a high-quality result and whose qualities and biases you understand[67] and know how to correct. Also ensure that you document the procedure used in your DPIA or in a procedure. If the DPIA is carried out by an external service provider, find out what methodology will be used and ensure that it is appropriate[68] .

[63] Risk detectability refers to an organisation's ability to identify and analyse the risks to which it is exposed. This variable is also referred to as the "level of control" in some methods.

[64] See, for example, the following passage in its deliberation No. SAN – 2025-015 of 22 December 2025 imposing a financial penalty on the company NEXPUBLICA FRANCE: "*... the company's inability to indicate which data were subject to breaches highlights the inefficient traceability of actions performed on the [processing]. The restricted panel recalls in this regard that it is recommended to provide for "active" traceability, i.e. to formalise a process for generating alerts and dealing with them in the event of suspected abnormal behaviour (see, in this regard, deliberation no. 2021-122 of 14 October 2021 adopting a recommendation on logging).*"

[65] Here are two concrete examples of detection measures that reduce risks: Many vehicles are equipped with an alarm that alerts the driver when one of the tyres is flat, helping to prevent accidents; the installation of smoke and/or CO2 detectors is required in many flats (according to the latest estimates, this requirement has saved 400 lives per year in France since it came into force).

[66] WP 243, revised and adopted on 5 April 2017

[67] See, for example, *Some limitations of qualitative risk rating systems*, by Louis Anthony Tony Cox Jr, Djangir Babayev and William Huber (published in June 2005 in the journal *Risk Analysis*)

[68] In the document *Survey on Data Protection Impact Assessments* published by the EDPS in July 2020, in the chapter entitled "*DPO involvement - How does the DPO get involved?*", I note the following passage: When DPIA *is outsourced to external service providers, there is a risk that they may not have the necessary knowledge and expertise and that the DPIA may not be carried out properly. For example, we*

2. **Once you have decided on your DPIA, you will illustrate it:** Do not insert a risk matrix into your impact assessment by convention, habit or imitation, but because you have decided to do so, after clarifying the objectives you wish to achieve.

3. **You will master the method of designing your illustration:** Many DPIA are produced automatically by tools designed for DPOs, mainly on the basis of a series of checkboxes. While this is undoubtedly a very practical aid for novice practitioners, it is essential that you take an interest in what lies beneath the surface and familiarise yourself with the algorithm imposed on you by the publisher. Do you know its principles, limitations and biases? Will you be able to explain to your data controller why the likelihood and severity of a feared event are assessed at such levels (or will you be forced to admit that you have no idea)?

4. **The value your illustration will create:** If the matrix adds nothing to the impact assessment submitted to the data controller, then it is useless. If you insert an illustration, it must serve one (or more) purpose(s) and create meaning and value[69] .

5. **Your approach must be honest:** The illustration you decide to include in your impact assessment should reflect a positive approach, helping the data controller to make the "right" decision in full knowledge of the facts, rather than attempting to conceal, downplay or present negative elements in a more favourable light, or trying to influence the decision. The role of DPO is often likened to a vocation, which can only be performed with a pure heart...

6. **Your illustration should be documented and explained:** Make sure you systematically provide (in an appendix to the impact assessment if necessary) the "instructions for use" for the risk matrix you have decided to include: What does each degree on the scales used for severity and likelihood mean? What method was used to position each risk on the matrix? At what point is a recommendation made to the data controller to seek the opinion of the persons concerned, or even the CNIL? etc. It is important to remain aware that the matrix *appears* analytical or even scientific, when in fact it is mostly based on an essentially subjective approach, i.e. that of experts.

7. **Pay attention to semantics:** The words that accompany your illustration are just as important as its structure. Therefore, choose them carefully so that they convey a meaning that is shared by all and are consistent with the risk assessment method used. In addition, it is good practice to include explanations or examples illustrating the qualitative scales.

8. **You shall proceed with several iterations if necessary:** It would be surprising to find the "right" formula for conducting your PFSA and illustrating it on the first try. You must remain humble and be able to question yourself. Every new process has its own quirks and problems that can only be

---

have found that some professionals, drawing on their experience in IT security assessment, are convinced that they can carry out a DPIA. However, this is not guaranteed, as experience shows that they encounter difficulties due to a lack of appropriate data protection skills.

[69] I highly recommend reading a scathing but thought-provoking opinion piece entitled *Faire une vraie analyse des risques cyber : guide critique d'un professionnel de terrain* (Conducting a real cyber risk analysis: a critical guide from a field professional). In it, Damien Peschet gently pokes fun at these "*reassuring matrices*". Selected excerpt: "*It is difficult to find a more universal symbol of risk analysis than the two-axis matrix. In meetings, it is a formidable tool: visual, concise, easy to understand. A single slide is enough to show that threats have been measured and that we know where to focus our efforts. This power of simplification is also its main flaw. The matrix creates an impression of objectivity that it does not have. The figures that position a risk on the grid are almost always the result of subjective estimates, influenced by the participants' perceptions, their past experience, or recent examples that come to mind. Two different teams working on the same scope can produce radically different matrices. The result is an attractive tool that is reassuring in form but, if misused, fosters a false sense of control. A well-presented matrix can convince a management committee that an organisation is in control, even when its actual defences are incomplete or obsolete. This visual veneer is sometimes more dangerous than a total lack of analysis, as it reduces vigilance at the very moment when it should remain on high alert*.

solved through continuous improvement. Get started and then iterate, taking care to review each impact analysis with a critical eye (try to put yourself in the position of an outside observer and take a step back).

9. **Ensure the sustainability of your matrix:** What could be more confusing than a matrix that varies with each impact analysis? Once you have determined the formula that suits you (and that everyone agrees on), stick to it. And if it is decided to have some impact analyses carried out by a service provider, make sure that the deliverables produced are not too far removed from what your data controller is used to.

10. **Present your illustration to the people concerned:** If the risk matrix were presented to the people directly concerned or their representatives, how might they react? Do they understand the illustration without needing your explanations? Do they agree with the ratings that have been assigned to each risk? Would they refuse to take risks (due to the processing) that are classified as acceptable in the impact assessment? This effort is all the more useful if your data controller is required to consult the CNIL under Article 36 of the GDPR, as the Commission will undoubtedly ask, "*And what do the data subjects think?*"

What type of matrix should I use?

Based on all of the above comments, I am now moving towards a 5x5 matrix, with the likelihood axis on the y-axis and the severity axis on the x-axis (Fig. 20). In addition to the fact that a fifth level offers greater precision in assessments, it allows *black swans* to be positioned if care is taken to devote the first level of the likelihood scale to the semantics "*It is conceivable, but highly improbable*".

In terms of semantics, I prefer the term "*likelihood*" to "*probability*" (which implies an analysis of observed frequencies and conveys an impression of scientific rigour that the approach cannot claim) and "*severity"* to "*impact*" (as an impact can be positive). The likelihood axis would include the following levels: "*It is conceivable, but highly improbable*", "*It is just possible*", "*It is possible*", "*It is entirely possible*", "*It is to be expected, it is certain*" - taking care to define each of these expressions. The Severity axis would include the following levels: "*Negligible*", "*Limited*", "*Significant*", "*Critical*" and "*Dramatic*". In my role as methodological guarantor, I take care to combat the natural tendency to want to position risks at the median value, in particular by attaching to my Delphi questionnaire a definition of each of the terms used, enriched with examples. Thus, the "*Dramatic*" level could be specified as follows: "*The feared event could prove catastrophic for those affected, or even irreversible (going so far as to indirectly cause their death). As a result of the treatment, those affected could experience significant, even irreparable consequences that they may not be able to overcome.*"

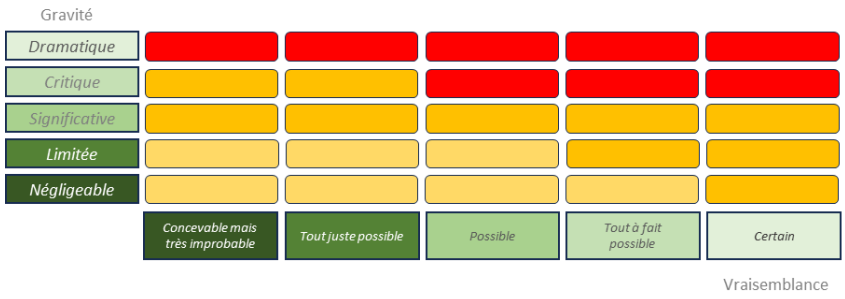

Figure 20: Proposed 5x5 matrix

I advocate the use of three colours: yellow, orange and red (avoiding green for the reasons mentioned *above*). They are arranged so that yellow and red never come into contact. The entire maximum severity line is coloured red, to be consistent with the definition of this level ("*even indirectly causing their death")*. Here is one possible configuration (Fig. 20), which must in any case be worked out with the stakeholders. It should be noted that the box at the top left (minimum likelihood/maximum severity) is

deliberately coloured in a more "alarming" colour than the one at the bottom right (maximum likelihood/minimum severity), even though their product is identical.

Imagine my surprise when I discovered in an AEPD guide[70] - which I had read when it was published in 2021 - a matrix very similar to the one I had come up with! Many thanks to Pablo Garrote Crespo, DPO of *Grupo Igualatorio Médico Quirúrgico* (IMQ), for pointing this out to me. As the table on page 97 of the Spanish document is presented with the axes reversed, I have reproduced it here for greater readability (Fig. 21). You will note the use of four colours (but not green), compliance with the rule that "extreme" colours should not touch each other, the fact that the entire top row is red, and that the boxes at the bottom right and top left are not coloured in the same way.

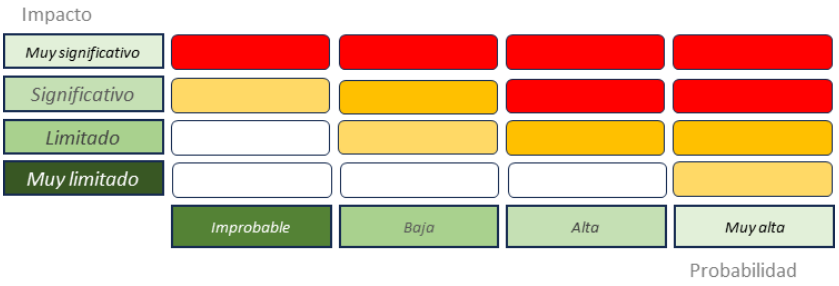

Figure 21: Table taken from the AEPD document

After consultation with the data controller, the next step is to set acceptable limits in order to define three zones (see example in Fig. 22). Zone 1 is known as the *prohibited* zone: there should be no residual risk in this zone. If this is not the case, an additional iteration must be carried out to add processing measures or reinforce the effectiveness of the measures already devised.

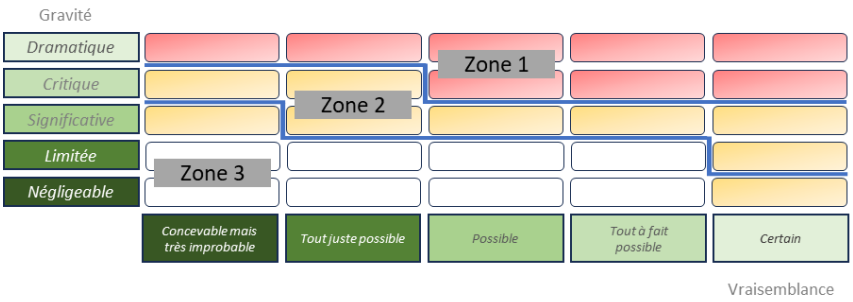

Figure 22: Addition of acceptability limits

If, despite this, risks still exist, the CNIL must be consulted in accordance with Article 36 of the GDPR[71] . The DPIA to be provided to the authority shall be accompanied by 1) an argument demonstrating that there are no other approaches that would achieve the purpose and present a lower level of risk to the data subjects; 2) a demonstration of the added value, societal contribution and/or benefit for the data subjects created[72] for [society/the community/the data subjects]; 3) a summary of the opinions of the data subjects or their representatives, as provided for in Article 35.9 of the GDPR. If the authority authorises the implementation of the processing, enhanced monitoring measures will be implemented in order to detect very quickly the possible occurrence of the feared events located in this zone. The residual risks positioned in zone 2 are endorsed, processed and monitored. Finally, those in zone 3 are monitored to verify that the assessment of their likelihood is relevant.

[70] *Risk management and impact assessment in personal data processing*, AEPD, July 2021

[71] And be prepared for a possible inspection (the CNIL may want to verify that the processing is not already operational).

[72] This concept is vague, which does not make it easy for data controllers to make decisions. In a workshop delivered in 2019 by CNIL agents to AFCDP members to present the PIA tool, we were told: "*For example, certain risks can be taken if the processing saves human lives. What are the benefits for individuals and the community? The answers to these questions enable us to assess the situation and determine whether the residual risks are acceptable. A balance must be struck between the residual risks and the challenges of the processing. Once the balance is tipped in the right direction, the PIA can be validated by the data controller, with acceptance of the residual risks.*"

Unsurprisingly, the debate will focus on the two extreme boxes, top left and bottom right. It is up to the data controller to decide whether the former is in zone 1 or zone 2 and to take responsibility for their choice (we cannot stress enough the need to have the data controller sign the DPIA). And customers who would be frequently impacted by a feared event positioned in the bottom right-hand box may be tempted to look elsewhere, even if the severity is negligible.

A call to tool publishers

No one was surprised to see GDPR tool publishers (originally focused on maintaining the processing register) expand their offering with a section allowing users to formalise a DPIA. Logically, they have all incorporated the method proposed by the CNIL (and implemented in the free PIA tool made available by the Commission), with all its advantages but above all its disadvantages. Having taken care to consult with several major players, I noted that they had nevertheless decided to eliminate one of the flaws in the PIA tool's graphical representation of risks, in particular by clearly delineating each box in the matrix. One of them went further, opting for its own semantics for the Likelihood axis (but kept those of the Severity axis). All made their own choices regarding colours, but above all their layout – with enormous differences: each publisher therefore imposes *its own* doctrine on the DPO regarding the limits of acceptability, which seems inconceivable to me. All of them told me that they followed this logic in order to help new DPOs, mainly those who are not familiar with technical matters (the approach being focused on cybersecurity aspects). This results in a litany of abstract questions, the answers to which lead to the positioning of three risks (and only three) on the matrix. This prevents a DPO who would like to identify several risks (for example, following EBIOS RM workshops) from doing so. While this may help a novice DPO (and no doubt reassure them), I believe that the adverse effects of this overprotectiveness are harmful, the main ones being: DPOs are forced to comply with a method that is imposed on them (and which may not necessarily suit them), an approach limited solely to the "cybersecurity" aspect " component, which results in ignoring risks that do not belong to any of the three proposed categories, and DPOs finding themselves alone in dealing with the AIPD and trying to answer the long list of questions.

Among the publishers I interviewed (thank you to them for their time), I found that only Dastra had introduced some initial degrees of freedom and gone beyond simply integrating the logic of the CNIL's PIA tool by allowing the "basic" matrix to be customised. In particular, the semantics and colours can be changed. In addition, an optional risk management module allows you to go further, in particular by adding rows and columns to the matrix and, if necessary, creating new types of risks (in addition to those relating to confidentiality, integrity or availability). This flexibility allows the tool to be adapted to the DPO's own approach to managing DPIA rather than forcing them to work within a rigid framework.

To meet the needs of experienced DPOs, I would therefore like to see these offerings enhanced to give practitioners more freedom to adapt them to their own approach (the GDPR does not impose any particular method for formalising a DPIA, as long as it meets the eligibility criteria). Here are the degrees of freedom that I consider desirable with regard to the risk matrix:
- Choice of the number of rows and columns (I would, however, keep Likelihood on the x-axis and Severity on the y-axis);
- Choice of semantics on both axes, and the possibility of customising the definition of each level;
- Choice of colours (allowing, for example, the green colour to be avoided);
- Choice of colour assignment for each cell (and, consequently, control of the "acceptability zones", with customisation of the definition of each zone);
- Option to create risk families (in addition to the three traditional ones relating to confidentiality, integrity and availability);
- Option to position several risks in each family;

- And therefore, the possibility of freely positioning risks on the matrix.

"A DPA that doesn't include a matrix is all too easily set aside without being read"

What do our colleagues abroad think? Several European DPOs to whom I sent an initial draft of this paper agreed to answer a few questions. Here are some very interesting responses:

Do you always use a risk matrix when drafting DPIA reports?

> "*As an external DPO, I mainly work with SMEs, some of which carry out processing activities that require a DPIA, such as video surveillance or profiling/analytical activities in the tourism sector. In these analyses, I generally include a risk matrix as a tool to facilitate the assessment process and, above all, to make the document more readable for the data controller.*" – Italian DPO.

> "*Almost without exception, I illustrate my DPIA reports with a risk matrix. It is, above all, an internal communication tool that helps make the document accessible and actionable for decision-makers, most of whom are not privacy specialists. In my experience, a DPIA that does not include one is all too easily set aside without being read … That said, I take care to present the matrix not as a standalone deliverable, but as a visual summary of a reasoned analytical process. The data controller must always be able to answer the following question: 'Why is this risk positioned here and not elsewhere?*" – Italian DPO.

If so, what are the characteristics of this matrix?

> "*The risk assessment method I am currently using is still under development and is being progressively improved. It is a highly complex tool that is not easy to implement in SMEs, as it requires specialist expertise which, in most cases, is unfortunately still lacking. Within a 5x5 matrix, I use a simple colour code that is easy to understand even for non-technical users: green (low), yellow (medium), orange (medium/high), red (high/critical). The thresholds are generally as follows, obtained by multiplying likelihood by severity: 1–4 green; 5–9 yellow; 10–14 orange; 15–25 red. "As for the colour green, I do recognise that it can trigger a typical psychological reaction of the 'everything is fine' variety, sometimes leading the data controller to consider that the risk has been completely resolved. This is an aspect I will look into, as even graphical elements can influence the perception of risk.*" – Italian DPO.

> "*We use a 4x4 matrix with three colours (green, yellow and red), but with a different layout to that seen in France: we colour only three squares red and, symmetrically, only three squares green, no doubt to prevent green and red squares from touching. And, indeed, this allocation places V4/G1 and V1/G4 risks on the same level and assigns them the same colour… which is strange when you think about it.*" – German DPO.

> "*My current standard is a 4×4 matrix, using the four-level ordinal scale derived from the CNIL methodology, which remains the main reference for Italian DPOs in the absence of a tool issued by our supervisory authority. I generally use three colours: green, yellow/orange and red. The Garante's guidelines do not impose any specific colour scheme, which leaves practitioners a certain degree of freedom. I add an acceptability threshold, which I consider essential: without it, the matrix cannot answer the crucial question of whether prior consultation with the authority under Article 36 of the GDPR is necessary. "For the semantic labels, I have moved away from the CNIL's symmetrical vocabulary, where the same terms are used for both axes. I find this conceptually imprecise."* – Italian DPO.

> "*I usually use a matrix with four rows and four columns, as well as four colours: red, orange, yellow and green.*" – Spanish DPO.

Were these characteristics defined independently, or do they stem from a specific tool or methodology?

> "*The characteristics of the matrix were defined independently, although they draw inspiration from several methodological sources: the CNIL's PIA tool, the ISO/IEC 29134 standard and ENISA's methodology for assessing the severity of data breaches. In Italy, no tool has achieved the level of market penetration enjoyed by the CNIL's PIA tool in France. Several tools offered to Italian DPOs include a risk matrix, but few (if any) allow for significant customisation of the semantics, choice and arrangement of colours, or acceptability thresholds*." – Italian DPO.

> "*In Bavaria, we mostly use the template suggested by our supervisory authority."* – German DPO.

> "*I am obliged to use the matrix imposed on me by the tool chosen by my predecessor, even though I sometimes feel it isn't suitable*." – Spanish DPO.

In your country, is there a 'standard' practice or are there different approaches?

> "*In my experience, there is no 'standard' practice regarding the risk matrix. However, there is a certain convergence on certain elements: 3x3 or 5x5 matrices, a distinction between gross risk and residual risk, and the use of colour to improve readability*." – Italian DPO.

> "*In Italy, there is no 'standard' practice for risk matrices in DPIA, as the Garante has not published a methodology or DPIA tool comparable to the CNIL's PIA software. One observation, however: many DPOs operate as external consultants serving several clients across different sectors. This creates a sort of 'standardisation', sometimes at the expense of the analytical depth required by a rigorous DPIA*." – Italian DPO.

> "*Although the Spanish Data Protection Authority has published a guide setting out examples that can be followed – though these are not mandatory – not all DPOs in Spain follow the same approach, and there are differences both in the structure of the templates and in the colours used.*" – Spanish DPO.

> "*In Italy, there is currently no standardised and universally recognised practice. The data protection authority has not published specific guidelines on the structure of the risk matrix in personal data processing operations, limiting itself to incorporating and referring to the WP29/EDPB guidelines. Consequently, different approaches are observed: in some cases, simplified matrices (3x3) are preferred; in others, more complex grids are adopted; some practitioners draw inspiration from risk management methodologies borrowed from the field of IT security (for example, ENISA's approaches), whilst others develop proprietary frameworks. There are also significant variations in terminology and the definition of risk levels."* – Italian DPO.

Is this topic the subject of discussion or debate within your DPO community?

> "*I get the impression that the matrix is still treated in a somewhat superficial manner, more as a 'document to be attached' than as a tool for genuinely improving the data controller's decision-making. In SMEs, this risk is amplified because the client's priority is often 'to fill in the document', whereas the correct objective should be to make the DPIA a tool for genuine governance. In far too many cases, unfortunately, not only the matrix but also the DPIA itself are approached with limited depth, being perceived more as a document to be produced than as a tool for genuine analysis of the processing*." – Italian DPO.

> "*The characteristics of the risk matrix as a tool are only very rarely the subject of debate within the Italian DPO community. The discussion tends to focus on procedural issues (when is a DPIA necessary? What must it contain?). A debate that is gaining momentum here concerns the relationship between DPIA's carried out under Article 35 of*

the GDPR and the fundamental rights impact assessments formalised under Article 27 of the AI Regulation: what impact this will have on the future of the methodologies currently in use. Italian AI law practitioners and privacy professionals are beginning to engage in an interdisciplinary dialogue in an attempt to find answers." – Italian DPO.

"*This issue has not yet received the level of attention it deserves within the Italian DPO community. There is still a lack of structured discussion that could lead to the identification of common best practices. I believe that greater standardisation – or at least the definition of common minimum criteria – would be desirable in order to ensure better quality and 'comparability' of DPIA reports, even though qualitative analysis remains an essential component of the analysis and must necessarily be adapted to the context.*" – Italian DPO

In conclusion (temporary)

I like to say that DPIA helps data controllers (and all stakeholders) to be concerned in an intelligent way, and that the risk matrices that illustrate our DPIA are valuable tools to help our data controllers make informed decisions. To paraphrase Mark Twain, they should not, on the contrary, lead them to underestimate the risks they have decided to impose on third parties ("*There are three kinds of lies: lies, damned lies and risk matrix ~~statistics~~*").

As I do not claim to hold the truth, I hope that this document will stimulate reflection and debate, particularly within the AFCDP, a French association that brings together and represents Data Protection Officers and, more broadly, any professional interested or concerned by compliance with the GDPR, and I look forward to receiving your feedback, suggestions and proposals in order to create an "ideal" representation of the risks for individuals.

A look to the future

Several proposals put forward in the Digital Omnibus would have a significant impact on the subject I have just discussed if they were adopted. The least significant of these is the publication of a single European-level list of categories of processing that require an impact assessment to be carried out. I admit that I was surprised that the authorities did not take the initiative to reach an agreement, particularly within the EDPS, to achieve this at the first attempt. However, the differences that currently exist between national lists seem minor to me. For example, Datatilsynet (the Danish authority) requires that "*processing operations for which a personal data breach could have a direct effect on the physical health or safety of a natural person*" be subject to an impact assessment. This corresponds to the category "*Health data processing carried out by health establishments or medical-social establishments for the care of individuals*" which appears in CNIL deliberation no. 2018-327 of 11 October 2018. It should be noted that the Danish list contains only eight categories, whereas the CNIL list contains fourteen.

There is another proposal that concerns me even more. The EDPS would be responsible for proposing a common model and harmonised methodology at European level for carrying out impact assessments. The wording of the Omnibus does not make it clear whether this methodology will be merely proposed or imposed. The GDPR currently describes what must be achieved by producing a DPIA (and the G29 guidelines list the criteria to be met), but does not impose any method for achieving this. I therefore hope that this will only be a suggestion, which will certainly be of great help to novice DPOs, but which will allow more experienced DPOs to continue to exercise their independence, including in their choice of approach.

If, on the contrary, it is an obligation[73] , several questions will arise, including the following: will it be necessary to "revise" DPIA already carried out to bring them up to the new standard? How long will it take for tool publishers to adapt... and at what cost to their customers? Will the CNIL's PIA tool be withdrawn or significantly modified?

I also fear that the single methodology will once again be a rehash of one of the risk analysis methods that is poorly (and rather badly) suited to impact analysis. I will not repeat here the points I mentioned *above*, but I fear that a method focused on cybersecurity will be imposed and that DPOs will be forced to adopt approaches that yield poor results. The lesser evil would be to see the EBIOS Risk Manager method selected[74] (Expression des Besoins et Identification des Objectifs de Sécurité), which is presented by ENISA as follows: "*EBIOS Risk Manager is a method for managing information security risks, created under the aegis of the French General Secretariat for Defence and National Security ( ), compliant with ISO 31000 and ISO/IEC 27005 standards, and enabling compliance with the risk management requirements of ISO/IEC 27001*."

Will we benefit from the work to be carried out by the EDPS to study the parts that could be shared in the event of the combined formalisation of a data protection impact assessment under Article 35 of the GDPR and a fundamental rights impact assessment[75] (or FRIA for *Fundamental Rights Impact Assessments*) under Article 27 of the European Regulation on Artificial Intelligence? I hope so.

The Digital Omnibus also proposes to exclude from the definition of data in Article 9 those that are currently included indirectly. This would be a step backwards from the CJEU ruling of 1 August 2022 (case C-184/20), which required that processing not only of intrinsically sensitive data, but also of data indirectly revealing such information through intellectual deduction or cross-referencing, be considered as processing of sensitive data. If this amendment is adopted, care must be taken not to take it into account when carrying out DPIA, at the risk of missing the obvious, as is already the case today with certain tools which, to make your life easier, simply raise a dozen or so questions before delivering a "turnkey" impact assessment. Among these questions is one about the presence (or absence) of so-called "sensitive" data (i.e. falling under Article 9.1 of the GDPR) in the data processing project. If we do not force ourselves to consider that innocuous data can become sensitive information in certain contexts, the result could be catastrophic. Any experienced DPO knows that the *sensitivity* of personal data is not only determined by its nature but can also be determined by context. For example, addresses are rarely included on lists of sensitive data, yet their disclosure can be very dangerous if they are disclosed. In the United States, actress Rebecca Shaeffer was murdered when a stalker obtained her address from the *Department of Motor Vehicles* (which manages driving licences). This tragedy led to the adoption of federal legislation on the protection of drivers' privacy, the *Driver's Privacy Protection Act*.

[76]Another project that could potentially have an impact on the implementation of DPIA and their quality: in order to streamline the procedures for reporting various "incidents" that organisations must report to different authorities in order to comply with several pieces of legislation (including personal data breaches that must be reported to the CNIL under the GDPR), a single European point of contact should be created

[73] In its document *Risk Management Standards - Analysis of standardisation requirements in support of cybersecurity Policy*, published in 2022, ENISA expresses the following wish: "EU policy makers should make certain risk assessment methodologies or tools mandatory for specific sectors, where necessary."

[74] In its analysis of the Digital Omnibus of January 2026, NYOB is in favour of this possible development: "*Overall, NYOB suggests adopting this provision as proposed. This suggestion would move away from the idea of a so-called 'risk-based' approach, with countless vague factors, where the data controller is largely left free to decide whether or not an article of the GDPR applies to them. Instead, this approach allows for a more objective and simpler application of the law, which improves legal certainty for all stakeholders.*" I confess that I do not know what this blissful optimism is based on, since at this stage we know nothing about the future methodology that will emerge from the EDPS's work... most likely another risk-based approach, with countless vague factors and where the data controller has the final say anyway.

[75] See *Fundamental Rights Impact Assessments: What are they? How do they work?*, EDPS, January 2025

[76] But not under the Artificial Intelligence Regulation.

to receive reports under the NIS 2 Directive, the DORA Regulation, the GDPR, the eIDAS Regulation and the Critical Entities Resilience (CER) Directive. This point of contact should be supervised by ENISA. This should eliminate the current disparity at European level between the information that must currently be provided by a data controller in the event of a personal data breach. However, it is possible that the new notification will be aligned upwards... and that it will be necessary to provide the DPIA that was (or should have been) carried out on the processing that was the subject of the breach. This is a good way to ensure that impact assessments are carried out and that they are conducted with the real objective of reducing the risks to data subjects.

Finally, the Digital Omnibus refers to the European Data Protection Board (EDPB) to formalise a list of circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of an individual. Let us hope that this deliverable will have a profound influence on the assessment of the level of risk in the context of a DPIA.

It is therefore to be hoped that the EDPB will listen to European DPOs on all these issues.

Dedication and acknowledgements

I dedicate this work to all DPOs who strive to do their job with perseverance, competence, integrity and independence.

Writing this document gave me the opportunity to exchange ideas with many fellow DPOs, including those abroad. Thank you to Pablo Garrote Crespo (DPO of Grupo Igualatorio Médico Quirúrgico), Charlaine Berendt (Group Data Protection Officer, Aenova, Munich), Nadia Arnaboldi (Vice-President of CEDPO), Massimiliano Pappalardo (Asso DPO), Andrea Repetto (Asso DPO) and Filippo Bianchini (Asso DPO). A big thank you also to Erik Boucher de Crevecoeur (CNIL), Patrick Blum (former General Delegate of the AFCDP), Jérôme de Mercey (co-founder of Dastra), Yann-Hervé Beulze (former RCCI, RSSI, DPO and Risk Correspondent at Groupama Asset Management), Christophe Champoussin (Anaxia Conseil, AFCDP Administrator), Edouard Schlumberger (co-founder of Leto), Alessandro Fiorentino (Adequacy), Mehdi Sbai-Idrissi and Benjamin Baratta (Witik) and Edouard Schlumberger (co-founder of Leto).

The author

Bruno Rasle describes himself as a "monomaniac" when it comes to GDPR compliance and practises this martial art in three ways: professionally, he has been a shared data protection officer for one of the branches of the French social security system, appointed for more than a hundred data controllers; as a volunteer, he is one of the very first members of the French DPO's association AFCDP and was its general delegate for a dozen years; finally, as a teacher, he is a lecturer in the oldest and highest-level training programme in Europe (he has been training privacy professionals since 2007). He also played an active role in creating the profession of Data Protection Officer in France (later Data Protection Commissioner). He is co-author of the following books: *Halte au Spam* (Stop Spam) (Eyrolles, 2003); *Correspondant Informatique et Libertés: bien plus qu'un métier* (Data Protection Officer: Much More Than a Job) (AFCDP, 2015); *Droit à l'oubli* (Larcier, 2015); *Se préparer au RGPD* (Éditions législatives, 2017). He created the AFCDP University for DPOs (and was its organiser until 2020), the AFCDP Index of Access Rights and the DPO Job Board (AFCDP). Bruno Rasle is the co-author of the DPO code of ethics and the annotated, commented and indexed version of the GDPR made available by the association. He participated in the creation of CEDPO (European Confederation of Data Protection Professionals), of which he was a board member.

He has published numerous articles, including "*The DPO: source of discomfort or creator of value?*", "*Communicating with victims of a data breach: going beyond the GDPR?*", "*Saving Private DPO!*", "*Is personal data security finally being taken seriously?*", "*EDPS report on the right of access under the GDPR: All that for this?*", "*GDPR rights requests: no form appears to be mandatory*", "*GDPR: They invented the machine gun for access rights requests*", "*The GDPR register is not an end in itself*", "*GDPR: Is this supervisory authority imposing unrealistic requirements?*", "*20 years of the AFCDP: memories, memories...*", "*Do you have to be paranoid to do a good PIA?*", "*Data purging – An effort that is well worth it*", "*For an ideal DPO appointment*", "*Courteline brings a smile back to DPOs' faces*", "*DPO colleagues: the annual review is a valuable tool; let's make it a best practice*", "*PSSI: constraint or opportunity?*"), as well as his conference presentations ("*Cookies and Widgets: can we really surf the web with peace of mind?*", AFCDP University 2011, "*Synergy between RSSI and CIL*", Cesin 2012; "*Compliance of Free Comment Areas*", AFCDP University 2013; "*Privacy by Design: the key role of developers*", AtoutFox 2013; "*CPO & CSO: Bridging the gap*", IAPP Brussels 2013; "*Are agile methods privacy-compatible?*", Cloud Week Paris 2015 "*Is Blockchain soluble in the GDPR?*", AG AFCDP 2017; "*The GDPR: evolution or revolution?*", JCAS Days 2017; "*What are we? Data controller? Joint controller? Processor?*", AG AFCDP 2019; "*How to audit your access rights management?*", AFCDP University 2021; "*Creating and running an RIL network*", AFCDP University 2022; "*Communicating a data breach to victims: going beyond the GDPR?*", AFCDP University 2025).

In addition to teaching on the ISEP Specialised Master's in "*Management and Protection of Personal Data*", the Oteria DPO Master's and the Panthéon-Assas DPO University Diploma, he offers short courses on behalf of Anaxia Conseil[77] ("*IT applied to the GDPR*", "*Conducting an Impact Assessment – From Theory to Practice*", "*Data Breaches: How to Avoid Them*", "*CNIL Audits – Preparing for, Managing and Surviving Them*", "*Being an Effective DPO from Day One*", *"Effective Management of GDPR Rights*").

[77] *www.anaxia-conseil.fr*