# User's guide to conducting a risk analysis and a DPIA using MONARC

## 1 Purpose of this user's guide

This user's guide describes how to conduct a risk analysis and a Data Protection Impact Assessment (DPIA) in order to meet the requirements of the EU General Data Protection Regulation (GDPR), more specifically regarding:

- responsibility and demonstration of compliance (Article 24),
- data security during processing (Article 32),
- the conducting of a DPIA (Article 35).

With regard to Article 35, the purpose of this user's guide is not to define the rules for determining whether processing is *"likely to result in a high risk to the rights and freedoms of natural persons"*, but to describe how to conduct out the actual DPIA.

With regard to the obligation to conduct a DPIA, the Article 29 Data Protection Working Party (G29) and a number of supervisory authorities have already issued guidelines.

## 2 Presentation of MONARC

### 2.1 Past history

MONARC (Méthode Optimisée d'aNAlyse des Risques CASES) has been in development since 2011; its aim is to enable very small, small and medium-sized businesses to manage the risks they face. MONARC is at one and the same time a method and a tool; it is user-friendly, providing the user with maximum assistance through knowledge bases, default values and information sharing.

CASES (Cyberworld Awareness Security Enhancement Services) is a department of the "Security Made In Lëtzebuerg" economic interest grouping, which goes by the name of "SecurityMadeIn.Lu". CASES was already well-known in the Grand Duchy in 2011, as it had been promoting information security since 2003, using themed campaigns and sessions to increase awareness among the general public, in businesses in the public and private sectors, and in fundamental schools in the Grand Duchy.

Like many risk analysis tools, MONARC was originally developed using Excel, but it was quickly moved onto an online platform in order to make it easier to share and circulate risk models. The "learning by doing" method is applied on order to develop the functions of the tool and the knowledge bases.

The constant presence of the CASES team in the field made it possible as early as 2014 to contact legal experts who were preparing the arrival of the GDPR. The evolutions of MONARC have been imbued with this since that date.

With a view to increasing the number of users and pooling contributions to the tool, MONARC was rewritten in an Open Source version in 2016, and is to be published on

GitHub in 2017. It can be downloaded from the site at github.com under "monarc-project" via a virtual machine offering the tool together with all its knowledge bases.

In 2016, another major step was taken with the Gäichel IX Joint Declaration in which the Luxembourg and Belgian Prime Ministers welcomed the start of collaboration.

The promotion of MONARC and its take-off are henceforth assured.

## 2.2 What is MONARC?

MONARC is a qualitative tooled method of risk analysis implementing ISO/IEC 27005. The choice of this international standard avoids exoticism and enables users to find a host of support materials.

MONARC manages information-related risks based on the "C.I.A." criteria (Confidentiality, Integrity, Availability). It proposes hierarchical modelling making it possible to visualise clearly the dependent relationship that exists between primary and supporting assets. Risks are calculated according to three criteria: the threat, vulnerability, and impact on the organisation. The choice of dissociating threat and vulnerability (rather than using scenarios) makes it possible not only to assess the risk in two phases, but above all to focus on vulnerability, i.e. the security measures in place and their deviation from best practices in this field.

In its basic version, MONARC offers two granularities for identifying risks:

- The optimised model is recommended for conducting the initial iteration of the risk analysis. It involves a pragmatic selection of the most frequent risks so that there is no side-tracking into futile details before the essentials are dealt with. These optimised bases have been created using the best practices in the field of information security and have been improved over time with the large number of analyses that have been conducted.
- The comprehensive model uses EBIOS knowledge bases, which allow an in-depth risk analysis that is extremely useful for successive iterations of risk analyses.

MONARC also manages operational risks. The difference between these and information security risks is that the impact criteria are based on the organisation's own values - "reputation", "operational", "legal", "financial", plus "personal" (impact on persons), all referred to here under the term "ROLFP". Operational risks are calculated according to two criteria: the likelihood of a risk scenario occurring, and the ROLFP impact. In this case, the choice of scenario makes it possible to describe business risks and governance risks more easily, in natural language.

MONARC offers knowledge bases that make it possible to identify the main risks in most contexts. A library of basic assets makes it possible to construct other more evolved assets, rather like a Lego construction. This hierarchical construction allows a very high level of customisation of the risk models, but what is most important is that each of the assets constructed in this way can be exchanged and improved between analyses and users: MONARC is thus a tool based on sharing and improvement.

# 3 Inventory of processing activities

The record of processing activities is the starting point for achieving compliance. It is therefore necessary to carry out an inventory of processing activities, if this has not already been done.

It is the responsibility of the *Controller* to decide which processing activities will be included in the DPIA.

It is important to adopt a pragmatic approach so that, depending on the size of the undertaking and the number and type of processing activities included in the impact analyses, it is possible to define the target of first the risk analysis and then the impact analysis.

In other words, it is necessary to check that the difference between targeting only those processing activities concerned and targeting the entire information system (or at least an entire functional sub-set) is not counter-productive. The MONARC methodology allows the re-use of risk analyses conducted in the past for transversal services or processes. Once one processing procedure or operation has been analysed, there is no need to conduct further analyses for the others.

Note: Conducting an information security risk analysis on a functional set of information or on an entire information system goes beyond compliance with the GDPR; it is a means of ensuring control over the security and continuity of your job activities.

# 4 Information security risks analysis

The MONARC risk analysis method offers a process that complies with ISO/IEC 27005. The tool guides the user through a succession of phases:

**Establishment of context**

This phase makes it possible not only to determine the perimeter of the analysis and define the elements the analysis will focus on, but also to define the reason for conducting the risk analysis. This information is crucial, as it affects the entire analysis and above all the use that is to be made of it (see below in the paragraph on the identification of assets).

During this phase, attention will be paid to the criteria for evaluating the risks, and more particularly to the impact table. By default, that table has a scale of values ranging from 0 to 4. This scale is commonly used; unless an undertaking has its own scale, it is therefore recommended that it - or at least the number of levels - should not be changed. In France, the CNIL advocates using a scale of four levels (not including 0). It proposes sufficiently generic titles for the levels; they only need to be copied in (if this has not already been done) and perhaps also contextualised to the organisation or its activity depending on the types of data being processed and the possible impacts on persons.

The phase of establishing context also makes it possible to focus on threats. In the specific case of the GDPR, the criterion of confidentiality is decisive, and any threat affecting this criterion must be taken into consideration. The criteria of availability and integrity are slightly less important, but again it is up to the Controller to decide

whether the risk analysis should be pooled to manage all the organisation's information risks or not.

**Identification of assets**

This phase makes it possible to accurately target the assets on which the analysis is to focus. In our professional jargon, we refer to "primary assets" or "business assets". They represent what is important for the organisation, namely its processes, its external services (such as an after-sales service), its internal support services (such as accounting, or management of human resources) and essential information, whether it relates to the business or to personal data. The information required for the processing of personal data must be included among these assets.

Modelling is extremely important. It is essential to have an accurate view of the data processing under consideration. Depending on which approach is adopted, it is possible to either omit data or include it more than once in the model, which could make it complicated or even inconsistent when positioning the impacts and consequences.

Explanations: Data may be processed within a service or within a process, but it may also be much more complex and affect the entire organisation. From experience, here are some guidelines when selecting which type of modelling to adopt:

a) Service-related view (internal or external): This view is relatively vertical (as in a stack) in the organisation's structure. Processing is carried out either internally in the various services, or transversally; it is precisely in this last case that its complexity increases. The processing activities are scattered across several functional services and business managers often have no knowledge of the workflow as a whole; it is therefore necessary to reconstruct and document the workflow, which is costly in terms of resources.

b) Process-related view: This view is by far the best. It coincides exactly with the organisation of jobs and the data processing carried out is very close to processing within the GDPR's meaning of the term. In all cases, the processing activities are described in sufficient detail, as are the related workflows, so that they can be modelled rapidly. Unfortunately, few organisations have an exact and documented view of their processes.

c) Information-related view: In this case, the analysis focuses on the data and the processing activities carried out. This approach is relatively simple, as is the resulting model; however, as the model does not correspond to a functional view of the organisation, the analysis cannot be used to process information-related risks. Pooling is complicated, and in some cases actually impossible.

Whatever type of modelling is chosen, consideration must be given to the life-cycle of the information (creation, use, archiving / destruction).

**Identification of impacts and consequences**

In the field of information security, the minimum security criteria are confidentiality, integrity, and availability. In MONARC, these criteria are directly linked to the ROLF consequences; these are generally decided on by the businesses and are then parametered at the level of the primary assets and inherited by the supporting assets.

Although this default inheritance allows some time-saving, it sometimes needs to be refined at the level of certain supporting assets.

**Identification of risks**

This phase is very much simplified in MONARC, since each supporting asset has an optimised risk model resulting from the requirements of Annex A of the ISO/IEC 27001 standard. The optimised model is based on the principal risks deduced from the absence of best practices in terms of information security. Modelling consists of describing the dependencies that exist between the primary and supporting assets. The knowledge bases included in MONARC allow the main risks to be identified; contextual risks have to be identified manually.

**Evaluation of risks**

In MONARC, risk is calculated according to three parameters: the likelihood of a threat occurring, its impact on the organisation, and vulnerability. At this point in the analysis, the probability of the threat materialising has been assessed during the "establishment of context" phase, and impact has been evaluated during the "identification of impacts and consequences" phase; all that then remains is to evaluate vulnerability in relation to the security measures already in place. This phase requires a level of competence common among practitioners in the field of information security. It is vital to have some knowledge of best practices in this field to be able to evaluate the measures in place. An expert in the field of information security should ideally conduct this exercise.

Once vulnerability has been assessed, the three parameters of the risk are entered, the value of the risk is calculated, and - depending on the threshold for acceptance of the risk - an indication in the form of a three-colour code (Green, Orange, Red) indicates whether the level of risk is acceptable or not. Red indicates clearly that the risk is unacceptable and recommendation(s) must be made to deal with it.

**Risk treatment**

Risk treatment consists of selecting one of the following four solutions:

- Acceptance of the risk: the risk is accepted in its current form, with no additional measures.
- Reduction of the risk: additional measures are put in place to reduce to risk to an acceptable level.
- Share of the risk: in the case of insurance, for example.
- Refusal of the risk: the cause of the risk is eliminated at source.

Risk reduction is the most frequently used type of treatment. Since the risks identified by default are based on the absence of best practices in terms of information security, MONARC offers for each of them between one and three security measures taken from the catalogue of best practices contained in ISO/IEC 27002.

For each risk, the effectiveness of the measures to be put in place must be estimated. This makes it possible to assess the residual risk, i.e. the risk that remains after the new security measures have been put in place.

This completes the risk analysis.

# 5 Analysis of impact with regard to information security risks

As already described, an Information security risks analysis focuses on the interests of the organisation, and mainly on the consequences that a loss of confidentiality, integrity or availability (C.I.A.) would have on the organisation's reputation, operation, legal or financial aspects.

The analysis of impact on persons focuses on the individual and the consequences a loss of confidentiality, integrity or availability could have on an individual's rights and freedoms.

In conducting the analysis of impact with regard to Information security risks, it is therefore sufficient to:

- make use of the Information security risks analysis, and
- parameter the impacts on the individual.

For calculating risks, MONARC takes into consideration the highest level of impacts, which should naturally be the case if an impact analysis is required

# 6 Analysis of impact with regard to legal compliance

## 6.1 Customisation of the basic model

The purpose of the analysis of impact with regard to legal compliance is to check that any failure to observe the requirements of the GDPR with regard to the rights of natural persons or the actual processing does not have a high impact on the rights and freedoms of natural persons. If this is the case, appropriate measures must be put in place to reduce the risks.

By default, MONARC contains a checklist arranged by theme that takes up the essential requirements set out in the GDPR:

- Two categories concern the organisation, and appear only once in the analysis:
  - Governance: This concerns keeping a record of processing activities, the consideration of "privacy by design" and "privacy by default", and the study of techniques such as the use of pseudonyms or encryption, etc.
  - DPO: This concerns the requirements regarding the need to designate a DPO and his/her minimum competencies and qualities.

- Seven categories concern processing, and are repeated as often as there are processing activities.
  - Principles regarding processing: purpose, transparency, excessive collection, etc.
  - Lawfulness and legitimacy: the conditions of lawfulness, obtaining consent, the specific categories of data, etc.
  - The rights of natural persons: all the rights of the person concerned (information, access, rectification, deletion, limitation, portability, and opposition).
  - Categories of data: a list of the categories of data involved in the processing.

- Sub-contractor: guarantees regarding safety, cooperation, 'cascade' sub-contracting, etc.
- Recipients: contractual clauses and the purpose of the processing.
- Transfer outside the EU: data protection, transfer clauses, etc.

It should be noted that all this information can be parametered and modified as much as desired. The checklist is no more than a starting point for checking the compliance of the processing. Depending on the desired granularity, the list should take the context into consideration and be adapted to suit the undertaking's needs.

Experience has shown that the list proposed by MONARC makes it possible to save a lot of time by focusing pragmatically on essentials. It is a starting point which, once evaluated, gives a fairly accurate idea of the state of compliance from a legal point of view. Accordingly, it is important to focus on weak points, then go on to adapt the comprehensiveness of the model depending on the sensitivity of the processing activities.

The list proposed by MONARC evolves as it is used; it is already possible to find a number of variants that may be integrated in the analysis using the models' import/export functions. Broadly speaking, although the categories mentioned above may take different forms, the basic content remains more or less the same.

Leaving aside considerations regarding language and form, and depending on context, it is possible to create a variant that makes the model more detailed and legible. This consists of not qualifying globally the three categories of data, sub-contractors, and recipients (of which there may be more than one) and using the free text field to list and describe them, but rather creating MONARC objects for each one.

In other words, taking the example of data categories, the exercise consists of creating in the MONARC library a "duration of conservation" object and giving it the name of the data category.

Thus in the example given above, the processing uses three categories of data: identification data, financial data, and lifestyle habits. For each of the three objects, the model will ask for the duration of conservation to be defined.

The main advantage of this modelling is that it centralises a defined list of categories of data applicable to all the processing activities. Whether to use a personal list or a list proposed by the control body is merely a matter of choice. To date, a number already exist, and they are of course all relatively similar.

The same adaptation is possible for sub-contractors. Rather than having a generic category in which the aspects of sub-contracting are described in general terms, one object should be created for each sub-contractor, named accordingly, and given the "sub-contractor" operational risk tag. This makes the qualification of each point of compliance in relation to sub-contractors more precise.

The same applies to recipients. Management is strictly identical to the management of sub-contractors: only the tag is different. It should be noted that if a company is both a sub-contractor and a recipient for two different processing activities, this needs to be reflected in the model.

There are not really any rules for defining the right model for a given context. It all depends on the complexity of the environment (number of suppliers, for example), the granularity desired, and the importance given to MONARC in providing proof of compliance.

### 6.2 Evaluation of impacts

The model of the checklist has now been defined. Each point of compliance must be assessed in the MONARC terminology, evaluating the risks of impact induced by each incidence of non-compliance.

The checklist is assessed in the operational risks part of MONARC. Before starting, it may be necessary to consider the option of whether or not to use "inherent" risks.

Explanation of the notions of "net", "residual" and "inherent" risk:

- "Net" risk represents the current status of the risk, taking into account the measures already in place.
- "Residual" risk represents the risk that remains after implementing the recommendations that have been made.
- "Inherent" risk represents the risk as if no measure had ever been put in place.

The choice of using "inherent" risk is one option. If the processing has actually already been set up, this option may be superfluous. On the other hand, in considering cases of implementing "privacy by design" for an innovative project, it is very probable that this notion of inherent risk will be pertinent. The notion is also pertinent for certain sectors of activity in the Grand Duchy.

In the part on operational risks, the risk is calculated according to the likelihood of the risk scenario and the ROLFP impacts referred to above. As the entry grid is fixed, it is necessary to focus on the impact on persons: the "P" column - impact on persons - needs to be filled in.

The method for completing the grid remains virtually identical to the method used for information-related risks, after assessing the likelihood of the scenario and the impact on persons. The risk is calculated and the risk situation must have been described factually in the first place. If the risk of non-compliance is too great, it will be necessary to deal with it by proposing recommendations for implementing measures that will reduce likelihood or reduce the impact on persons. For operational risks, this granularity is at the level of each risk, which allows better contextualisation.

# 7 Analyse of impact with regard to operational risks (businesses and organisation)$$

There may still be one category of risks that has not been treated. These are business-related risks - risks specifically related to the data-processing covered by the impact analysis. These are generally strategic or organisational risks that may have an impact on the person concerned, for example further to a failure in a data workflow, or the lack of a decision, or incompatibilities in the processing activities.

There are no knowledge bases at this level: the risks are too closely related to the context. However, all the preceding phases can be used as support.

### 7.1 Using models of risk analysis

Business risks are parametered according to the model of information risks at the level of primary assets. If the service- or process-based model has been selected, it is highly likely that no new object will need to be created. The process-based view is by far the most suitable in this context. An organisation that has knowledge of its processes surely has the maturity to describe the corresponding business risks.

If the analysis is conducted on the basis of "privacy by design", the task is more complicated.

In all cases it is very easy to create containers representing processes, services or processing activities that present specific risks.

There are two ways of creating risks:

- Creating single risks on the fly for each object
- Creating "Tags - Operational risks" and then allocating objects to these tags, since certain risks are the same for a number of processing procedures or operations.

Note: Operational risks must be formulated negatively due to the absence of best practices, inappropriate security level, insufficient resources, gaps in processing, etc. It is then possible to evaluate the scenario on a scale of 1 to n: the higher the value, the more plausible the scenario.

### 7.1 Evaluation of impacts

The evaluation and treatment of business risks are carried out in exactly the same way as for the checklist of legal aspects, with or without the parametering of "inherent" risks.

Regarding compliance with the GDPR, only the "P" column (impact on persons) has to be filled in. If the analysis is also to be used for the organisation's risk analysis, the ROLF columns also need to be filled in; MONARC takes into account whichever impact is greater.

# 8 Finalisation, proof and iterations

### 8.1 Consolidated treatment plan: list of measures to put in place

Whether it is for a risk analysis regarding information or the three types of impact analyses, all the recommendations made for dealing with major risks and incidences of non-compliance are grouped together in a single treatment plan.

In terms of visibility and transparency, the treatment plan is vital, as it makes it possible to centralise all the actions to be implemented in order to achieve compliance. The plan is transcribed in full in the final deliverable.

MONARC also makes it possible to follow implementation of the treatment plan, to add the names of people that are responsible, the deadlines allowed, and various comments documenting the proper performance of all the actions intended to achieve compliance.

### 8.2 Results and proofs

Currently, the deliverable supplied by MONARC is directed towards risk analysis and is not immediately adapted to delivering the elements that are relevant for an impact analysis. The information is, however, delivered already formatted in Microsoft Word, which makes it quick and easy to customise the deliverable.

MONARC is Open Source software: it is highly likely that a GDPR-dedicated deliverable will be programmed at some point.

Based on my experience of information security certifications, choosing to propose that auditors have direct access to the MONARC analysis makes their work easier and quicker. It creates a feeling of transparency which is always welcome when an audit is being conducted.

### 8.3 Iteration

MONARC is a tool which uses an iterative method to manage risks. It will therefore naturally update your analyses periodically in line with the DPIA, which, we should recall here, is a process.

## 9 Conclusion

Conducting an impact analysis requires competence on two levels: it has legal aspects, and it involves information security. These are two different worlds with two different approaches, but they have essential complementary competencies.

Therein lies the entire issue of tools designed to help with a compliance project. Most of the tools available on the market are actually generalist checklists of compliance points; this is not at all suitable in the field of risk management, which is far too complex to be modelled in a two-dimensional spreadsheet such as Excel.

The advantage of MONARC is that it is designed to manage information risks and operational risks. By design, it incorporates the notion of impact on persons and checklists of compliance.

It is a good compromise, and costs nothing: it therefore ought to be adopted.

**Thierry Petitgenet**, GRC Consultant (Governance, Risks and Compliance)

Founder GRC-Luxembourg.

www.GRC-Luxembourg.lu