Position Paper

FERMA
Federation of European Risk Management Associations

Av. de Tervuren, 273 B12
1150 Brussels, Belgium
T: +32 (0)2 761 94 32
F: +32 (0)2 771 87 20
E: enquiries@ferma.eu
www.ferma.eu

# FERMA's Views on the Guidelines on Data Protection Officers Adopted on 13 December 2016 by the Article 29 Data Protection Working Party

15 February 2017

The Federation of European Risk Management Associations (FERMA) is supportive of the work by the Article 29 Working Party and welcomes the Guidelines on Data Protection Officers (DPOs) released in December 2016. FERMA, whose member associations represent more than 4700 risk managers in a wide range of European business sectors, believes they will prove a valuable tool to understand the implications of the General Data Protection Regulation (GDPR) for their day to day activities and facilitate its compliance.

**FERMA recommends that the Guidelines refer to an Enterprise Risk Management (ERM) methodology in order to ensure a professional approach to the assessment of data protection risks.[1] We further believe that the "three lines of defence model" (see below) is likely to be relevant in this process and could be updated to the latest cyber law requirements, including the GDPR and notably the new function of DPO.**

FERMA has consistently stated that cyber/information security is an enterprise-wide risk and compliance with the GPDR cannot be the sole responsibility of the IT department. An important part of the risk manager's role is to conduct a careful and thorough risk assessment of the activities of the organization, including likelihood and impact levels as well as financial exposure. Such an enterprise-risk management approach allows the proper identification, analysis and evaluation of the risks, and this applies to digital risks such as data protection.

**Professional risk managers share some of the key features of the DPO as described in the GDPR. FERMA believes that the role of DPO does not necessarily need to be a newly created function.**

Because there is no suitable governance in place to manage this evolving risk, FERMA set up a joint project with the European Confederation of Institutes of Internal Auditing (ECIIA) to develop a set of recommendations on corporate governance processes that will support organisations in managing cyber risks across their operations.

The participants of this joint working group are risk managers and internal auditors from eight EU countries (Belgium, Bulgaria, Denmark, France, Germany, Italy, Spain and UK) and six economic sectors (banking, defence, transport, food services, IT and telecom). The outcome of this project will be published in June 2017 in Brussels.

[1] There are two generally accepted international framworks/proceses for enterprise risk management :

- ISO 3100 Risk Management
- COSO ERM

## FERMA makes the following recommendations regarding the Guidelines on Data Protection Officers

### Point 3.5 Conflict of interests

*"*[…] *The DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data* […]*"*

FERMA agrees with the need to provide the DPO with a certain level of neutrality and independence from the personal data processing activities.

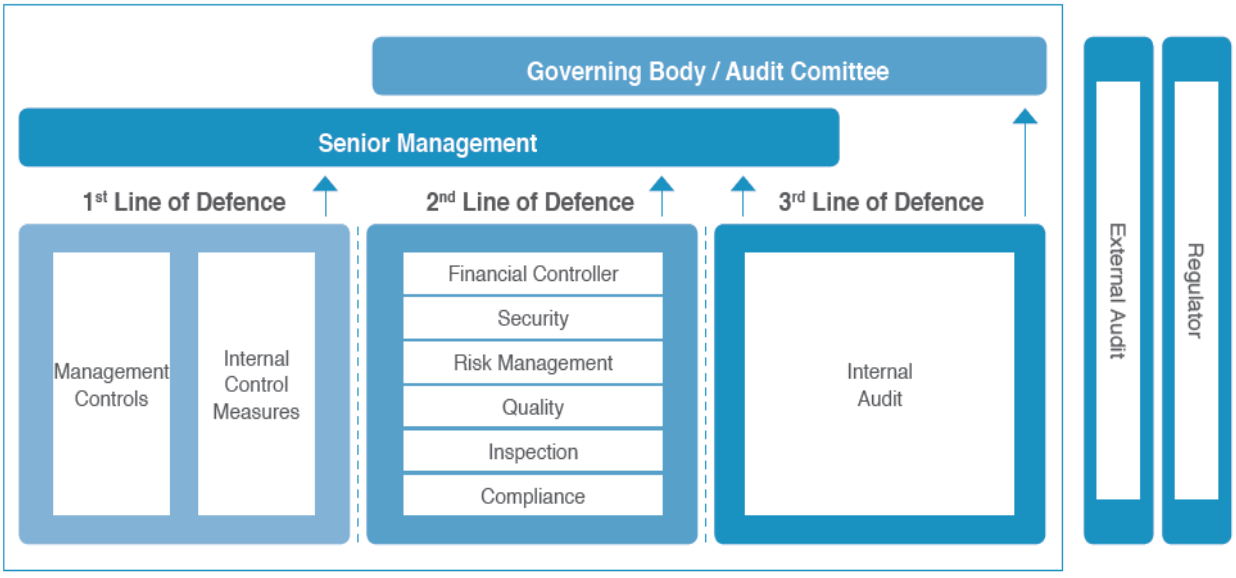
We are convinced that a sufficient separation of the DPO from IT is also necessary to ensure that cyber risk management strategies remain aligned with the business strategy and objectives.

FERMA believes that the three lines of defence model[2] could be a useful help to explain clearly where the DPO should sit and should be included in the Guidelines.

In this model,

- Operational functions involved in determining the purposes and means of the processing of personal data form the first line of defence.
- The risk management function acts in the second line of defence and
- Internal audit functions as a third line of defence.

In FERMA's view, the DPO function belongs in the 2nd line of defence in this methodology:




[2] See page 10 http://www.ferma.eu/blog/2014/10/ferma-eciia-respond-corporate-transparency-requirements-launch-new-guidance-document/

**Skills and knowledge required**

It seems that no profession currently has the necessary set of skills and knowledge to perform the DPO function, i.e. the "*expert knowledge of data protection law and practices and the ability to provide advice as regards the data protection impact assessment*".

Nevertheless, professional risk managers share some of the key features of the DPO as described in the GDPR:

| DPO key features in the GDPR | Risk manager's key features |
|---|---|
| *"The data protection officer shall directly report to the **highest management level** of the controller or the processor " (art 38.3)* | Two-thirds of risk managers **report to the board or top management level**[3] |
| *"The data protection officer shall be bound by **secrecy or confidentiality**" (art 38.5)* | Confidentiality is the **3rd core principle of the FERMA Code of Ethics** for risk managers[4] |
| *"The data protection officer shall in the performance of his or her tasks have **due regard to the risk** associated with processing operations, taking into account the nature, scope, context and purposes of processing" (39.2)* | An important part of the risk manager's role is to conduct a **thorough risk assessment of the activities** of the organization. It combines both **likelihood and impact** levels as well as financial quantification. The enterprise-wide risk management approach allows the proper **identification, analysis and evaluation** of the risks. |
| *"[…] To provide **advice** where requested as regards the **data protection impact assessment**" (art 39.1 c.)* | |
| *"The Data Protection Impact Assessment (DPIA) shall contain at least an **assessment of the risks** to rights and freedom and the **measures** envisaged to the risks…"* | Once the risk manager has properly assessed the risks following the ERM**Error! Bookmark not defined.** principles, he/she is able to suggest several types of **responses to put in place**, including **prevention and protection measures** to reduce the risk exposure to an acceptable level. |

FERMA therefore believes that the role of DPO does not necessarily need to be a newly created function. It could be exercised by other existing positions in the organisation, notably the risk manager, with some adjustments and thus avoiding an extra cost layer.

## Point 4.3. Risk-based approach

*"*Article 39(2) […] *requires DPOs to prioritise their activities and focus their efforts on issues that present higher data protection risks"*

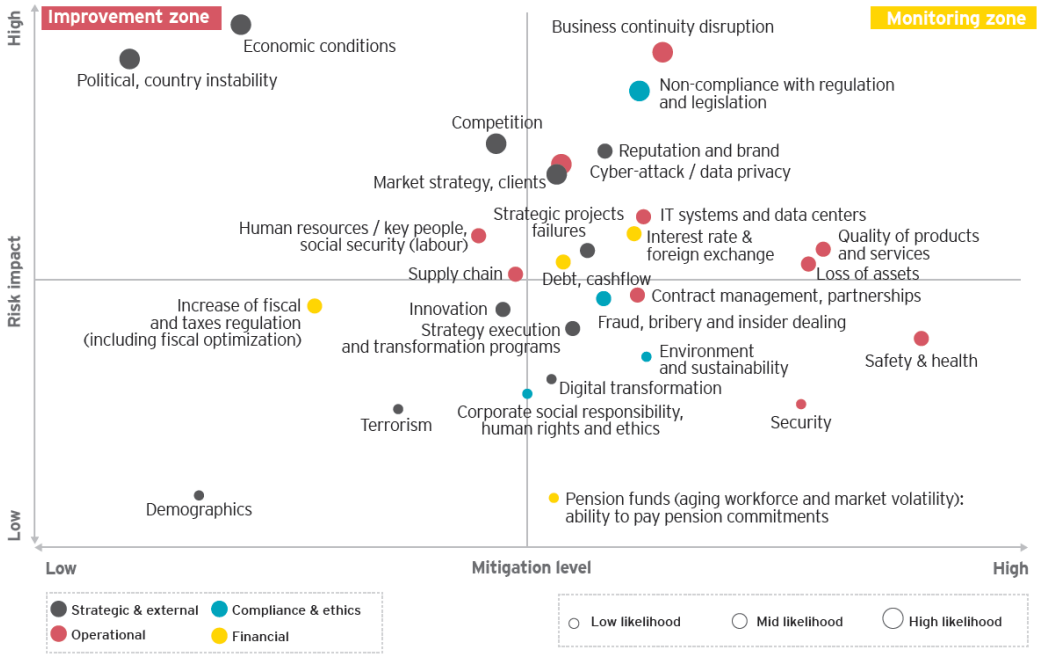
In risk management terminology, the task of prioritising activities and focussing on higher data protection risks is considered as a risk mapping exercise. Risk mapping is an element of the ERM methodology, commonly applied in large organisations.

Risk mapping helps to define models for the assessment of the frequency and impact of the risks identified. Once the mapping has been performed, risk matrices are developed to provide a visual

[3] 8th European Risk and Insurance Survey (October 2016) conducted by FERMA http://www.ferma.eu/blog/2016/10/risk-managers-developing-strategic-role-wider-view-risks-survey-finds/

[4] See rimap code of ethics at http://rimap-certified.org/wp-content/uploads/2016/05/Rimap-Code-of-ethics.pdf

understanding of the risks and their relative weights. They are particularly relevant for the risk-based approach promoted in the DPO Guidelines.




*Risk map in the FERMA European Risk and Insurance Report 2016*

## Conclusion

FERMA therefore recommends that the Guidelines refer to the ERM methodology[5] in order to ensure a professional approach in the assessment of data protection risks. We also consider that the three lines of defence framework, updated to make it relevant to the latest cyber laws requirements, may be effective in the implementation of the GDPR and notably the new function of DPO.

[5] There are two generally accepted international framworks/proceses for enterprise risk management :

- ISO 3100 Risk Management
- COSO ERM

## Contact person

Julien Bedhouche, FERMA EU Affairs Adviser, julien.bedhouche@ferma.eu

## About FERMA

The Federation of European Risk Management Associations brings together 22 risk management associations in 21 European countries, representing more than 4700 risk managers active in a wide range of organisations. FERMA provides the means of co-ordinating risk management and optimising the impact of these associations outside their national boundaries on a European level.

Member associations are from the following countries: Belgium (BELRIM), Bulgaria (BRiMA) Czech Republic (CZRMA), Denmark (DARIM), Finland (FinnRima), France (AMRAE), Germany (GNVW), Italy (ANRA), Luxembourg (ALRiM), Malta (MARM), Netherlands (NARIM), Norway (NORIMA), Poland (POLRISK), Portugal (APOGERIS), Russia (RusRisk), Slovenia (Sl.RISK), Spain (AGERS and IGREA), Sweden (SWERMA), Switzerland (SIRM), Turkey (ERMA) and United Kingdom (Airmic).

FERMA is a member of the International Federation of Risk and Insurance Management Associations (IFRIMA). www.ferma.eu