What to expect from a GDPR Assessment

Performing a GDPR Assessment is the first step any business should take before the regulation comes into force in May 2018. Metaphor IT will help you to understand the key risks facing your business under the General Data Protection Regulation and help you decide which threats you need to mitigate against and how you can do this.

The General Data Protection Regulation is all about protecting personally identifiable information of staff, clients, suppliers and anyone else you hold information on, so this is not just about the technology you use but also the processes in place within your organisation – the GDPR defines this as technical and organisational measures.

Our assessment is broken down into five sections:

1. Identify the risks

- We will work with you to identify risks associated with availability, confidentiality and integrity of data.
- Identify and document the effect that losses of availability, confidentiality and integrity might have on your business.
- For each risk, we will help you to identify the risk owner.

2. Assess the risks

- Once identified, we will then assess the impact and harm the business might have from the loss of availability, confidentiality or integrity, for each of the risks.
- We will then assess the realistic likelihood that each of these risks might occur.
- A decision is made, for each of the risks, as to whether it is acceptable or if it must be controlled in line with criteria established in the General Data Protection Regulation. Our process documents this in table format, highlighting the severity of risk using a red, amber, green methodology.

3. Identify and evaluate options for the treatment of risks

- For each of the risks, we then identify the possible options for treating it in line with the decision made in the assessment of risks.

4. Report

- We will present our findings to you in a thorough report, documenting areas of concern and suggested remedial actions and timeframes.
- For each of the risks, we'll discuss treatment actions with you, categorising each risk as accept, reject, transfer or control. We'll determine where responsibility lies within your organisation for remediation.

5. Select control objectives and controls for treatment of the risks

- Following the report, appropriate control objectives will be selected or designed according to the specific needs of the risk and the organisation. Controls to achieve those objectives are selected from a variety of sources.
- The final selection of controls and control objectives and the reasons for the selections (whether inclusion or exclusion) will be documented. Any risk the business determines as disproportionate to treat must be documented, clearly stating the business reasons for such a decision.
- Implementation of control objectives will be clearly defined, managed and documented throughout its implementation lifecycle.
- Once implemented, these control objectives and controls are then summarised in the documentation.