Nigel Gooding & Ademola Adekunbi

UK GDPR
&
Data Protection Act (2018)

RISK MANAGEMENT

Nigel Gooding & Ademola Adekunbi

WHAT DOES RISK MEAN TO YOU?

RISK/HAZARD

- A data protection risk is the likelihood (high, moderate, low) that somebody could be harmed by these hazards, together with an indication of how serious the harm could be to the data subject and the organisation.

- A data protection hazard is anything that may cause a data breach or harm. *Sensitive personal data of employees left on a manager's desk overnight.*

So, is risk management an art or a science?

RISK BASED APPROACH

Article 39(2) - ‘have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing’.

What does this mean?

- This article asks for a common-sense approach.
- DPO’s to prioritise their activities.
- DPO’s advise the controller on methodology.
- To be used consistently (ROPA, DPIA, Individual Rights…)

EXPLICIT REQUIREMENT

Article 5 - “The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘Accountability’).

What does that look like?

Article 25 – Data Protection by Design and Default

Article 32 – Security of Processing

Articles 33 & 34 – Data Breaches

Article 35 – Data Protection Impact Assessments

CONTROLLER OR DATA SUBJECT?

We are measuring risk to the data subject within the confines of state of the art, costs of implementation of appropriate organisational measures.

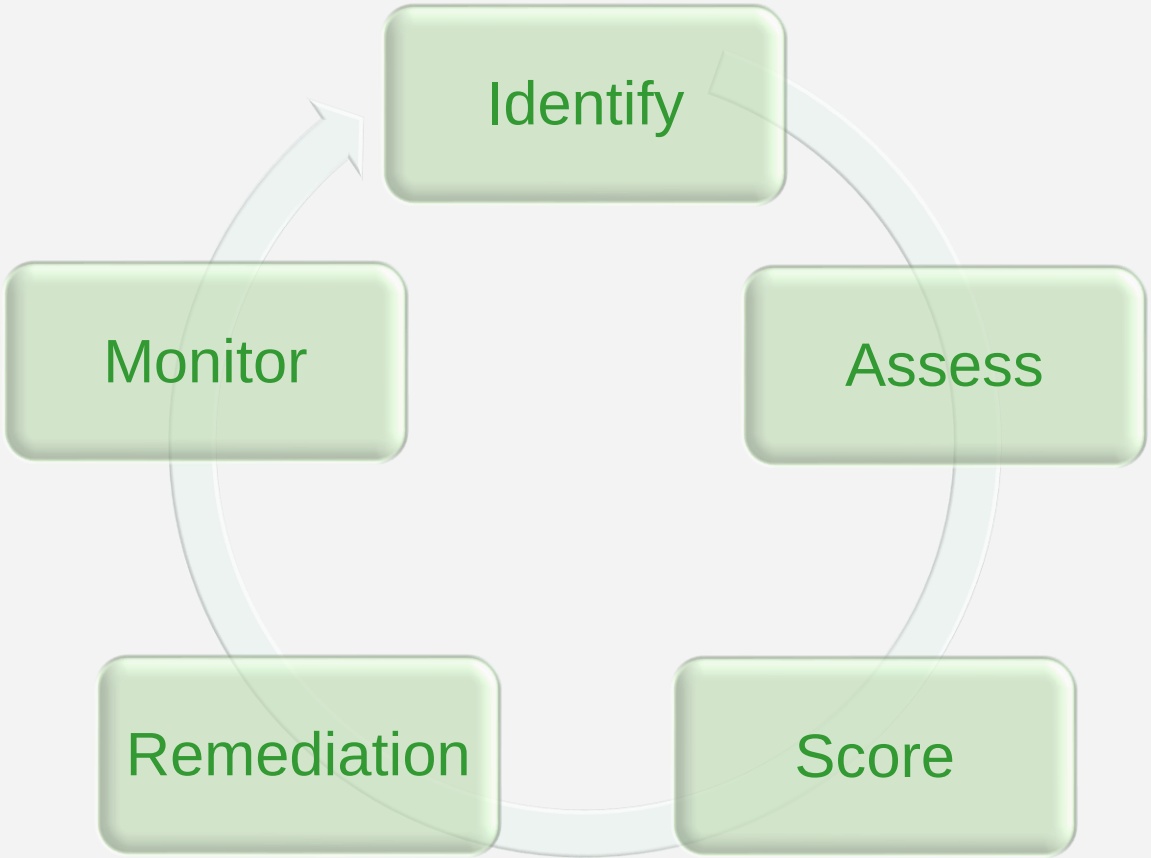
GDPR requires us to assess the risks to the data subject of actions of the data controller.

The requirements do not require the controller to have in place gold plated solutions.

It is a balance, and this is where risk management comes in!

RISK CYCLE

RISK CYCLE



RISK MODEL

Scores of **16 – 25** – **High risk** instant action required.

Scores of **8 - 15** – **Moderate risk** – action required and remediation within 1 week.

Scores **1-7** – **Low risk** – assessment of remediation require, if any.

How might you remedy the risk?

- Remove the risk altogether.
- Change the likelihood.
- Change the consequences.
- Share the risk through agreements, partnerships, further insurance etc.
- Retain and mitigate the risk by informed decision.

DATA SUBJECT IMPACT	SCORE
Not Serious Basic personal data such as name and business email address/job role. Shared within the organisation or to professionals with a duty of confidentiality. Personal data that is in the public domain. Non-traceable. No provable financial loss. No reputational loss. No physical loss. No loss of service. **(No special category data)**	**1**
Mildly Serious **Externally released.** **A larger number of data subjects.** **Location of breach/destination of personal data.** Low-risk personal data like children's/minors' personal data (13 - 18), relationship data, and gender. Unlikely to have a **significant impact** on the data subjects. No financial loss. No physical loss. No loss of service. **(No special category data)**	**2**
Fairly Serious **Externally released.** Details may include special category data (for example health data, depending on the context, including who it was disclosed to). A high volume of data. The number of data subjects affected. Consider proportionality; the higher the proportion of data subjects affected, the higher the risk. May include contact details and data that is classified confidential May include special category data of children. Financial data - credit card details and verification details (risk of fraud). Criminal convictions data. May have to notify the ICO. Provide data subjects with an open flow of communication. **(Any risk involving special category data is automatically deemed fairly serious - entry level 3)**	**3**
Serious **Externally released.** Details will include special category data (for example, health data, depending on the context, including who it was disclosed to). Special category data of children. Data that is classified restricted, classified or secret A high volume of data. The number of data subjects affected. Consider proportionality; the higher the proportion of data subjects affected the higher the risk. Contact details, including names and addresses. Financial data - credit card details and verification details (risk of fraud). Passport details and visa (right-to-work details). Criminal convictions data. Individuals are potentially at risk of harm. Action may be required as there is evidence this may impact individuals' rights and freedoms. Will have to notify ICO. Provide data subjects with an open flow of communication.	**4**
Extremely Serious **High risk to data subjects.** Details will include special category data. Special category data of children. High volume of data shared. Large number of data subjects affected. Consider proportionality; the higher the proportion of data subjects affected, the higher the risk. The party who has accessed/received the data is unknown, or a high risk individual/organisation. Criminal convictions data. Individuals are at risk of harm. Immediate action is required as there is evidence that this will impact individuals' rights and freedoms. ICO will have to be notified, including the data subjects.	**5**

CONTROLLER IMPACT

Not Serious
Small numbers of Data Subjects affected. Likely to be an internal risk
No loss of service.
Data Classification: Public data - in the public domain
(No special category data. However, if external then the entry point is mildly serious)

Mildly Serious
Small numbers of data subjects affected or low risk personal data. External.
Unlikely to have a **significant impact** on the data subjects.
No financial loss. No physical loss.
(No special category data)

Fairly Serious
Larger numbers of data subjects affected, internal or external and would have some impact on data subjects.
Details may include special category data and data that is classified confidential
Likely to result in enforcement action and potentially Tier 1 or 2 fines, and potential claims for compensation from data subjects.
Remediation costs for breach Low - Medium
Reputational damage - Low-Medium
(Any risk involving special category data is automatically deemed fairly serious - entry level 3)

Serious
Large or small numbers of data subjects affected, internal or external.
Likely to have a significant impact on data subjects and may include special category data.
Likely to result in enforcement action and potentially Tier 1 or 2 fines and compensation claims from data subjects.
Remediation costs for breach - Medium to high
Reputational damage - Medium to high

Extremely Serious
High risk to data subjects, potential that the organisation is unable to function due to a breach or a stop processing notice.
High risk of Tier 1 or 2 fines or stop processing notices, large or high number of compensation claims from data subjects.
Remediation costs for breach - High
Reputational damage - High

PROBABILITY	SCORE
Unlikely to occur	1
May possibly occur. Remediation work can be delivered quickly.	2
Likely to happen. Remediation not identified, funded or planned. Medium term implementation period.	3
Very likely to happen. Poor controls in place. Remediation plan not in place.	4
Very likely to happen soon or has happened. No controls or remediation plan in place or if plan is in place, long term delivery timescale.	5

EXERCISE 1 – Data Breach

An HR employee could not find her briefcase, which contained his laptop and papers related to staff sickness files. The employee told her manager that he believed the laptop was encrypted and the paper files were redacted. The manager reported the incident to the IT department, who remotely wiped the laptop.

What is the risk and the probability score?

EXERCISE 2 – DPIA

In order to create resilience within the team you have been asked to review a DPIA whereby GPs can provide virtual triage services from home. The local CCG are providing a secure VPN link from the Doctors home to the live surgery environment and will be providing data secure laptops on which Doctors only are able to login via biometric data. To compliment the new working practice Doctors will be required to adhere to a policy that they work alone in a secured room whilst at home.

What are the proposed risks?
Discuss them on your table and then provide me with a score

THANKS FOR ATTENDING

Does anyone have any questions?

info@dataprivacyadvisory.com
0203 301 3384
www.dataprivacyadvisory.com