www.pwc.com/mt

# GDPR
# The role of the Internal Audit Function

24 May 2017

pwc

## *What should the Internal Auditor do?*


... it's not your problem ... *yet*

## How does GDPR feature in your 2017 audit plan?

***"much of 2017 will be taken up with GDPR readiness and testing."***

Audit&Risk
Insights from the Chartered Institute of Internal Auditors

# ... during the next 12 months

## *Risk Assessment*

The features of business that are most affected by the GDPR:

- Consumer facing activities
- Activities relating to children
- Marketing and advertising
- Digital transformations
- Geolocation
- Profiling
- Tracking
- Public services
- Mass communications
- Joint ventures
- Global business operations

***Are we ready?***
***Will we be ready?***

## Policies

- Data classification policy
- Data retention policy
- Information security policy
- Privacy policies
  (corporate; staff; online)

***Are we ready?***
***Will we be ready?***

## Procedures

- Privacy by design
- Privacy by default
- Privacy Impact Assessments
- Consent management
- Subject access requests
- Breach notification
- Data portability
- Right to be forgotten

***Are we ready?***
***Will we be ready?***

## Contractual terms with:

- Employees
- Suppliers
- Clients
- Processor (liability)
- Controllers
- Binding corporate rules

***Are we ready?***
***Will we be ready?***

Gap analysis → Project implementation

- Processing Activity Register
- IT systems changes
- DPO in place
- Training programme
- Data cleansing
- Consent documentation
- Website updates / cookies
- Privacy notices

## ***12 months pass quickly***

***...*** *except if you're in jail*

*Today, have we got:*

- Awareness at board level?
- Awareness at first + second line?
- Buy-in from key stakeholders?
- A DPO?
- A budget?
- Roles, responsibilities, accountability?
- Expert help if we need it?
- ... a plan?

The Internal Audit function needs to keep the Aud Comm aware of progress with the steps being undertaken by the organisation, highlighting any delays and emerging risks that need to be addressed.

## *This time next year …*

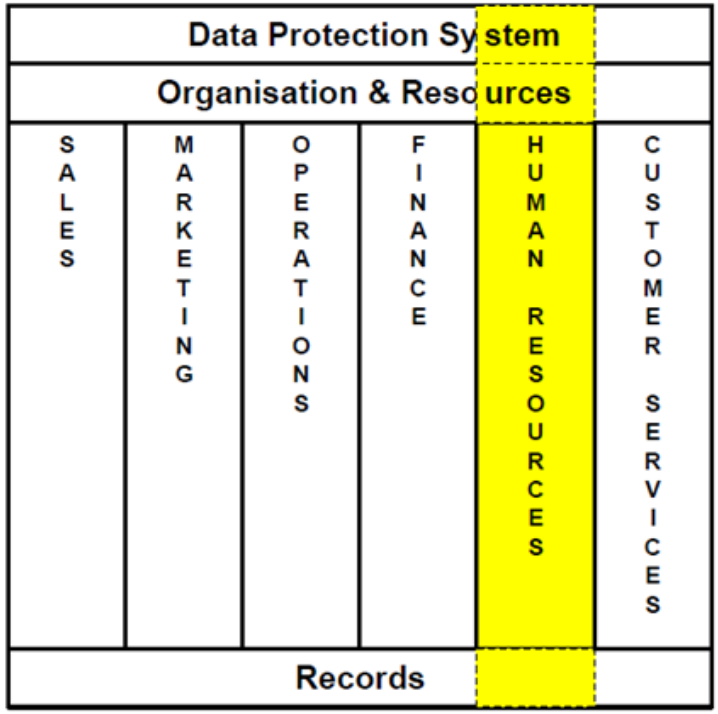
## *Privacy Audits :*
## *- Adequacy Audit*

To check that any documented Policies, Codes of Practice, Guidelines and Procedures meet the requirements of the GDPR.

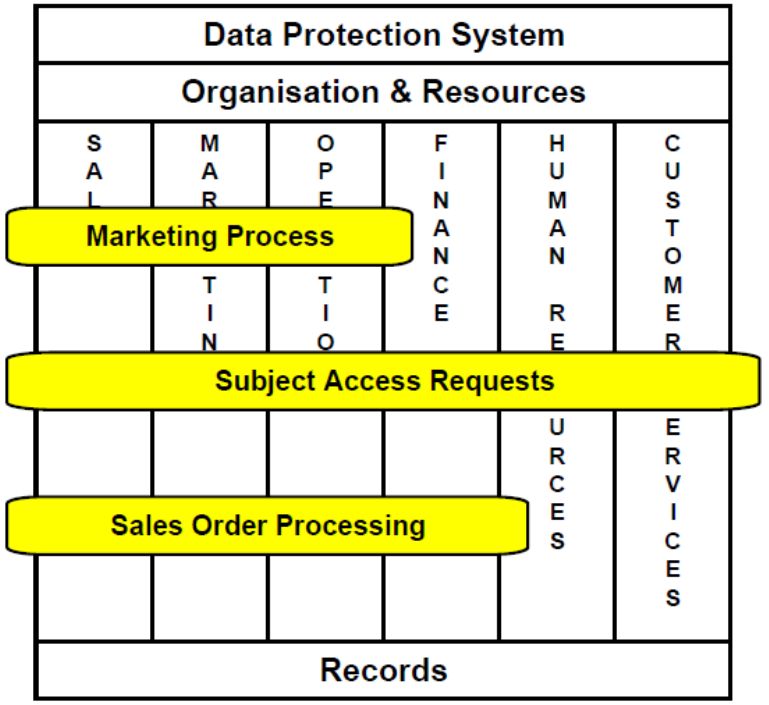
- May be extended to cover other legal requirements linked to confidentiality or data processing
- Work programme = checklist of GDPR obligations

## *Privacy Audits :*
## *- Compliance Audit*

To check that the organisation is in fact operating in accordance with its documented Policies, Codes of Practice, Guidelines and Procedures




Functional (vertical) audit




Process (horizontal) audit

## *Privacy Impact Assessments*

When using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

Most relevant when:

- there are special kinds of data (sensitive)
- Large scale processing
- Profiling / automated processing

***Plan to scale with software***

***Embed DPIAs into the first line of defense***

## *DPO Role*

***Data protection officer*** *- Important projects need owners. Under the GDPR, a data protection officer (DPO) is supposed to be responsible for creating access controls, reducing risk, ensuring compliance, responding to requests, reporting breaches and even creating a good data security policy. Businesses will need someone to act as the focal point in ensuring compliance with the GDPR and businesses will need to appoint DPOs sooner rather than later.*

ARTICLE 29 DATA PROTECTION WORKING PARTY

*Hopefully there will also be some liaison between the DPO and Internal Audit!*

## *Commercial Benefits?*

- Doing the right thing with personal data can enhance brand values
- Data quality improvements – quality and consistency of Management Information should improve
- Getting consent right early will allow your firm to use data where others may not
- System updates / consolidation reducing long term IT spend
- Will make it harder for unregulated firms to enter the market and take a share
- Avoidance of fines / reputational damage for non-compliance


***How we react positively to enforced changes can make a real difference, particularly in a crowded marketplace.***

## *The journey*

| | |
|---|---|
| ***1. Analyse*** | What data will you process, how and why? |
| ***2. Risk Assess*** | What are the risks and what harms can be caused? |
| ***3. Consult*** | Which stakeholders do you need to consult with? |
| ***4. Design*** | How will you built in data protection from the beginning of processing? |
| ***5. Document*** | How will you prove compliance? |
| ***6. Engage*** | What information should you give to the public and what consents do you need? |
| ***7. Challenge*** | How will you handle incidents, problems and complaints? |
| ***8. Supervision*** | How will you handle the application of legal rights and supervisory powers? |
| ***9. Sanctions*** | How will you cope with the most serious regulatory sanction and civil litigation? |


24 MAY 2018