



Enabling the  
information society

# GDPR for Quality Managers

EurIng **Carol Long** CEng FBCS CITP MCQI CQP

BCS Chartered Institute of IT, Northampton

30 January 2018

# Agenda

- Introductions
- GDPR Legislation and Timeline
- Practical Discussion
- Summary
- Q&A

# About Carol Long

Some projects that give a flavour:

- 1985 working on a “customer data” project that was result of first Data Protection Act
- 1998 developing international ERP software and supporting products for business data around second Data Protection Act
- 2007 education sector project to report workforce (personnel) data for UK national planning
- 2015 working with charities on CRM (customer relationship management) as GDPR became relevant

Visiting Fellow at Warwick University, Board Advisor for Risk and Audit, consultant and author

# About You

- Student or Academic Staff?
- IT specialist, IT or Quality Manager, other manager?
- business, education, public sector, NFP, other?
- Data Protection Officer, done GDPR training, not looked at data protection regulations yet?

# Agenda

- Introductions
- **GDPR Legislation and Timeline**
- Practical Discussion
- Summary
- Q&A

# A little Data Protection history

1950 Council of Rome, Privacy is a fundamental right

1984 UK Data Protection Act

1995 EU Directive 95/46/EC

1998 UK Data Protection Act (based on EU Directive)

2012 EU Commission review of data protection and privacy

2016 EU General Data Protection Regulation (GDPR) in force, 2 year compliance period begins from 25 May.

2018 EU GDPR will be enforced for all organisations worldwide from 25 May.

# Scope of GDPR

- Protection of Personal Data for all EU citizens, residents, workers and those travelling through EU
- Worldwide jurisdiction – it is the data that is EU
- Regulation exactly the same in all EU states superseding previous laws from 1995 Directive
- some local enhancements because of other regulations (e.g. Germany)
- UK introducing own legislation, very similar
- Other countries probably adopting EU approach
- BRexit is not applicable nor a “get out of jail”

# Easy Language Definitions

- Personal Data – about a real living person, that can identify them, includes biometrics, voice and image
- Consent – an informed agreement for personal data use
- Sensitive Data – personal data that could be used to discriminate or harm (e.g. sexual preferences, medical records, race, religion)
- Filing System - electronic or paper, organised/structured
- GDPR Notice – an instruction to comply or face further action
- GDPR Order – equal to a court order against you & fine
- Fine – up to 4% of annual turnover of parent company or Euro 20,000,000



# GDPR Who is Who

- Data Subject – the person the data is about
- Data Protection Officer – person appointed by an organisation to be principal advisor and auditor within the organisations
- Data Controllers – responsible organisation for storage, use of data
- Data Processors – may host data or deliver mailshots. Now in scope!
- Supervisory Authority – the government agency who acts to enforce GDPR e.g. in the UK a very helpful Information Commissioners Office (ICO)

# The Person's Rights

Direct control of use, retention, and movement of own personal data

- Understand how data about them will be used in detail
- Have a real choice about giving their consent or opt out
- Know data held about them is accurate
- Know that data about them is held safely and can't be misused
- Know when data about them is lost/stolen/moved
- Know that data about them won't be held indefinitely
- Right to be forgotten = right to erasure
- Portability = transfer of their data for their convenience
- Free access to complete records held on them (30 days)
- Right to sue, damages if data lost/misused in own country

# An Organisation's Obligations

- Transparency about personal data collected, stored, use
- Get *informed* Consent to have/use the data
- Protect the data
- Restrict Access – need to know only, logged
- Security of data - monitor and report breaches
- Transfer from/to third parties when requested by subject
- Suppliers – check personal data transferred/received complies
- Give access (free) to complete records for a data subject on request
- Have a point of contact (e.g. Data Protection Officer)
- Notify regulator and data subject of breach within 72 hours

# Optional bit for Smaller Organisations

- Appointment of Data Protection Officer  
(if processing smaller data volumes of non-sensitive personal data)

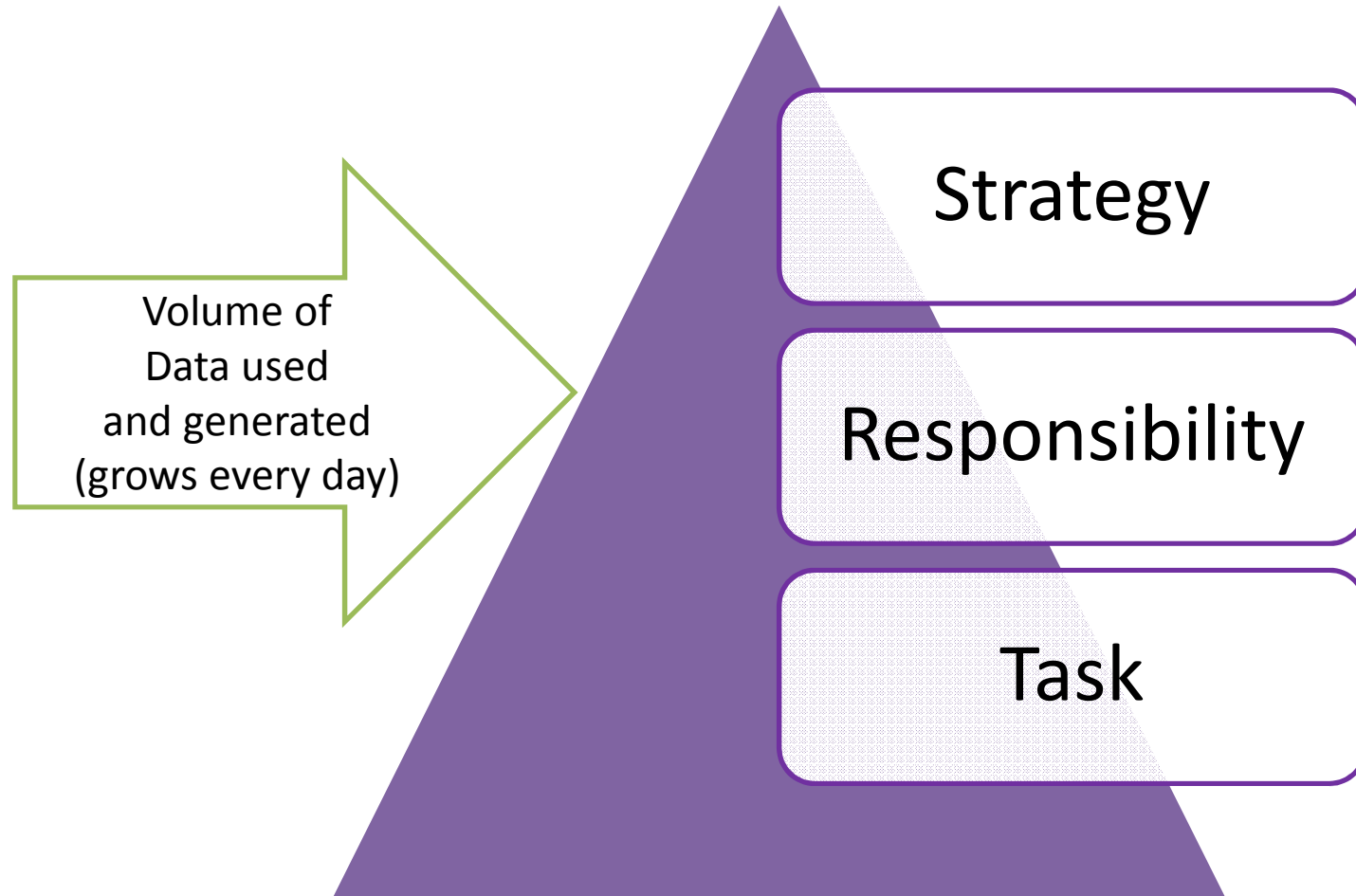
**BUT a quality manager may ask:**

- Who will keep everyone on track and be expert advisor?
- Manage the correspondence from ICO (or others)?
- Who will manage the Data Subject requests?
- Who is monitoring for and responding to breaches?
- Who is keeping it on the senior management agenda?
- What happens when they are on holiday?

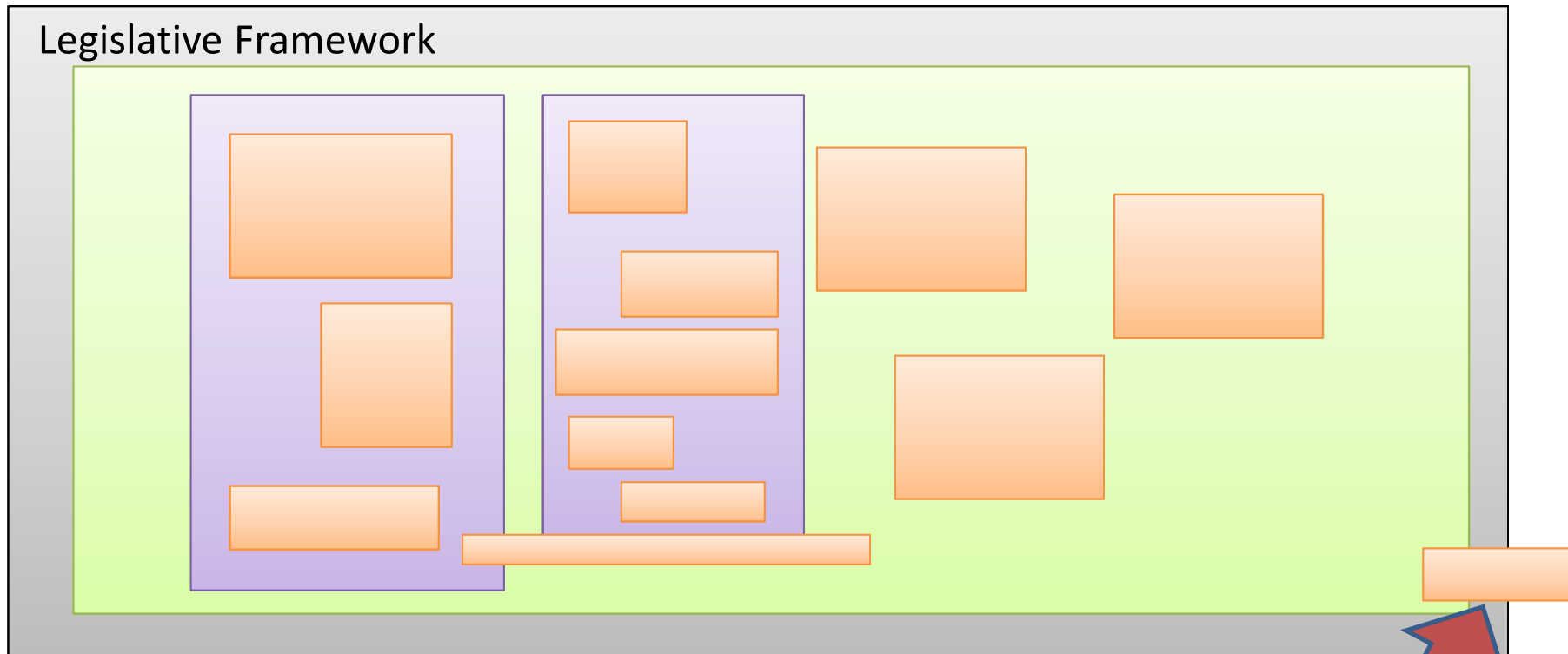
# Agenda

- Introductions
- GDPR Legislation and Timeline
- Practical Discussion
- Summary
- Q&A

# About Organisations' Data



# Business Data is Often Disjointed



Organisation level – corporate governance, common data



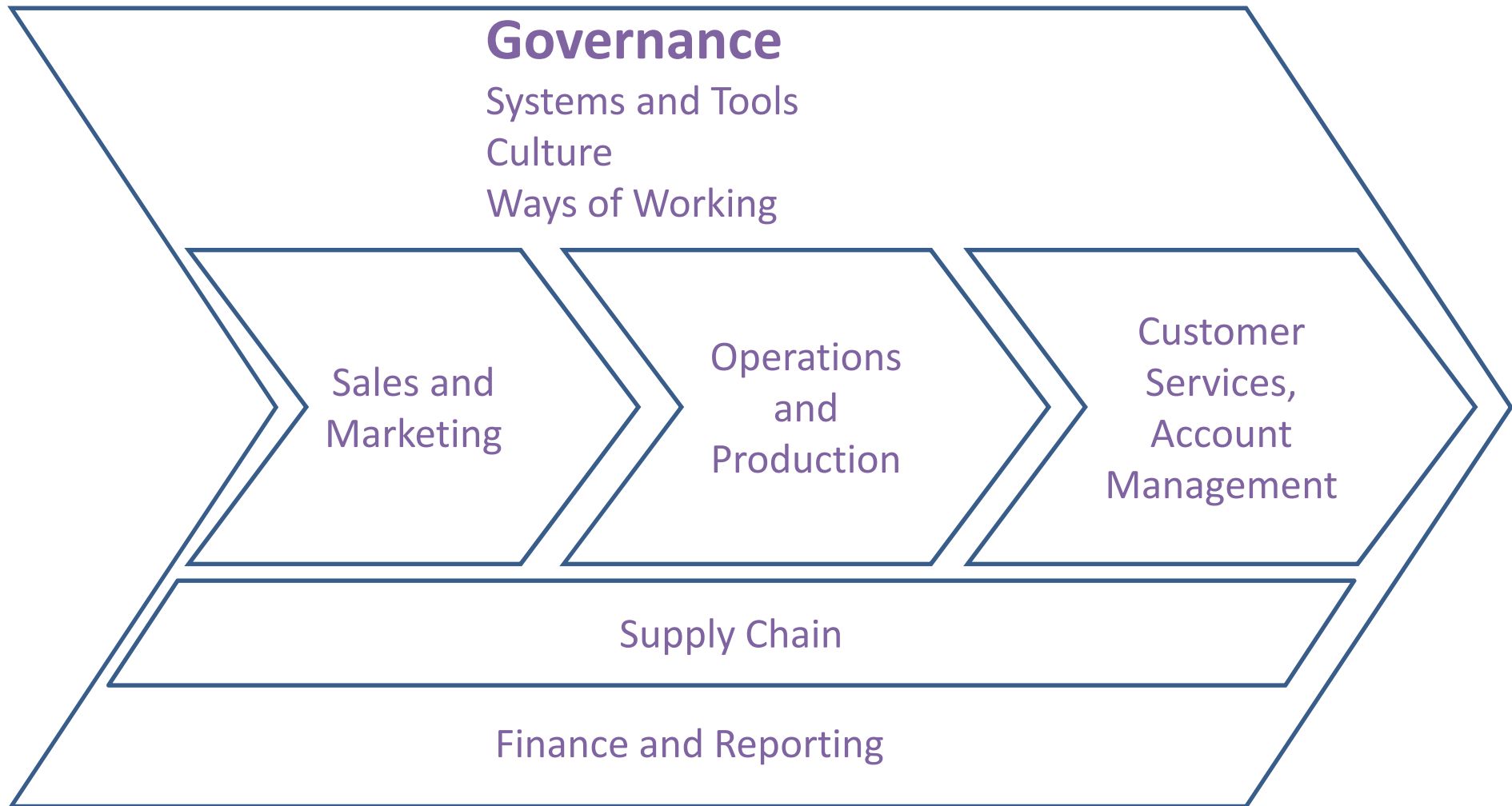
Programme level – programme or projects data



Team level – standalone projects, “technical” or task data

BYOD users side gig

# Its not an IT Problem!





# Quality Manager's Role?

- Support managers understanding GDPR needs
- Assist Data Protection Officers understanding of unfamiliar processes
- Question effective implementation of data security fundamentals
- Explain the reputational damage and fines risk
- Promote a customer data focus
- Check training happens for all
- Changes thinking from tasks to system data flow
- Practical action to support digitalisation
- Support for project teams
- Ask what is the minimum personal data we need?

# Agenda

- Introductions
- GDPR Legislation and Timeline
- Practical Discussion
- **Summary**
- Q&A

# Summary

- GDPR Legislation effective 25 May 2018
- Applies worldwide for protection of personal data of those who live, work or is a subject of an EU country
- Fair and Lawful processing of personal data must be the focus
- not much time to fix messy business data use
- Extended rights: protection and access control, erase, transfer/portability, transparency of use, information requests
- Fines will be large to encourage compliance (not breaches only)
- Potential benefits for customers and business efficiency
- Need to change behaviours; quick fixes are problematic if personal data used, workaround is probably non-compliance
- Suppliers are upgrading software
- Quality has a role to support DPO, question projects/managers
- **Prepare Now! Orders and Fines will start 26 May 2018**



**Questions?**

# Thank You

GDPR for Quality Managers

Carol Long CEng FBCS CITP MCQI CQP

BCS Chartered Institute of IT, Northampton

30 January 2018