IMS Health & Quintiles are now IQVIA™

Mini Summit 2 - EU General Data Protection Regulation (GDPR) Privacy Update

IPC

May 15 , 2018

Agenda

- Panel introductions
- General introduction: GDPR
- Expert insights
- Questions and answers

European General Data Protection Regulation (GDPR)

A New European Regulation Coming Into Effect On May 25, 2018

Directive 95/46/EC

Data Protection directive with regard to the processing of personal data and on the free movement of such data – transposed to member state laws

Replaced By

GDPR

Regulation directly effective in member states without the need for implementing legislation.
Fully in force from May, 25,2018 in all EU countries

- Stronger rights for Individuals
- Greater accountability requirements
- Increased Scope
- **Strong sanctions and penalties for non-compliance: top fine is up to 4% worldwide group turnover**

What Are The New GDPR Requirements?

Select Requirements under GDPR

Right to data erasure/ restriction

Information systems need to support the discovery of data about a person and be able to evidence its removal or restriction

Right to data access/ portability

Data must be retrievable and provided in a structured and commonly used electronic format. Vendors may need to comply with requests as well.

Data retention

Technology systems must be able to track data expiry and evidence that appropriate data archiving or expiry has taken place.

Data breach

Organizations must be capable of identifying breaches and impacted individuals, as well as support communications to those individuals.

Accountability

Maintain inventory of all processing including transparency of supplier arrangements to controller customers. Capability to demonstrate compliance in internal and external audit.

Consent

Where consent is required to process data, organizations must have systems that can provide mechanisms to capture, store and manage consents to validate and evidence compliance.

Data Protection Officer

DPOs are expected to be tech savvy and proficient at managing IT processes and data structures and proactively engage in the review of systems.

Embed data protection

Data protection requirements must be designed into business processes, products and services from the beginning and assessed and documented when necessary.

GDPR Applies To Organizations That:

- Are established in the EU and process personal data
- Are based outside of the EU and process personal data of data subjects residing in the EU

IMS Health & Quintiles are now

IQVIA™

Nicola Orlandi

Learnings and challenges – DP roadmap

- **Enabling responsible and sustainable use of data**

- Privacy by default and by design in practice: DP assessment and mapping, third party management
- Risk assessment and management: All parts of the business need to live up to their accountability for responsible data use in order to drive compliant innovation
- Risk and control self assessment to enable business to effectively identify and mitigate risks
- Definition of a standardized and integrated approach across the company
- Transparency: Contract templates and notice templates

- **Enabling creation of value through use of personal information**
- Design innovative strategies that consider responsible data use, enabling innovation and sustaining health systems
- Statement about definition of personal information meaning /choice of legal basis/digitalization and big data/AI etc...

Questions

1. What is the main impact of GDPR in the daily activities of a pharma company? And on scientific research?

2. What is the added value of GDPR for individuals and for a pharma Company?

IMS Health & Quintiles are now

IQVIA™

Willy Vanbuggenhout

GDPR - What is changing?

Accountability

Harmonization

Mandatory Data Protection Officer(s)

Broader territorial scope

Data Breach notification

Extended rights & protection for individuals

Increased fines & enforcement

- Applies throughout the EEA (i.e., EU + Norway, Iceland and Liechtenstein)
- May apply outside EEA ("offering goods & services" or "monitoring online behavior")

Privacy, Legal, JJT, with business engagement, defined a risk based plan

Policy & Procedure

- Updates to Framework, privacy notices and consent forms
- Policy updates for non digital commercial activities
- New Global Breach Notification and Escalation process
- Data Protection Impact Assessment (DPIA) process
- Documentation of processes supporting compliance

Data Protection Officer (DPO) / Governance

- Identification of company Data Protection Officer (required by regulation)
- Creation of Data Protection Officer team (leveraging existing Privacy resources)
- Creation of steady state GDPR Governance model

Third Party Contracts/Data Transfer Agreements

- Updates to contract guidance and template language
- Updated inter-affiliate data transfer agreement
- Integration of privacy evaluation into Business Partner Risk Assessment
- Remediation of contracts

Awareness and Audit

- Awareness and communication to business
- Internal audit, testing & monitoring strategy and plan

Systems Remediation

- Regulation translation to high level JJT requirements
- Identification of in-scope websites, mobile applications and business applications
- Remediation of websites and applications

Enabling Technology

- Tool for Data Protection Impact Assessment and Records of process activities
- Update to Business Partner Risk Assessment Tool

GDPR Risk Profile

GDPR increases risk:

- Substantially higher fines
- More coordination and collaboration in enforcement
- Data subject rights allow for more “activist” enforcement
- Notification of breach requirements increases visibility to regulators
- Uncoordinated country guidance undermines harmonization
- Late guidance from authorities and complexities of implementation will result in full implementation beyond May
- Legal uncertainty in certain areas remain: e.g. cross-border data transfers
- Other countries mimic GDPR

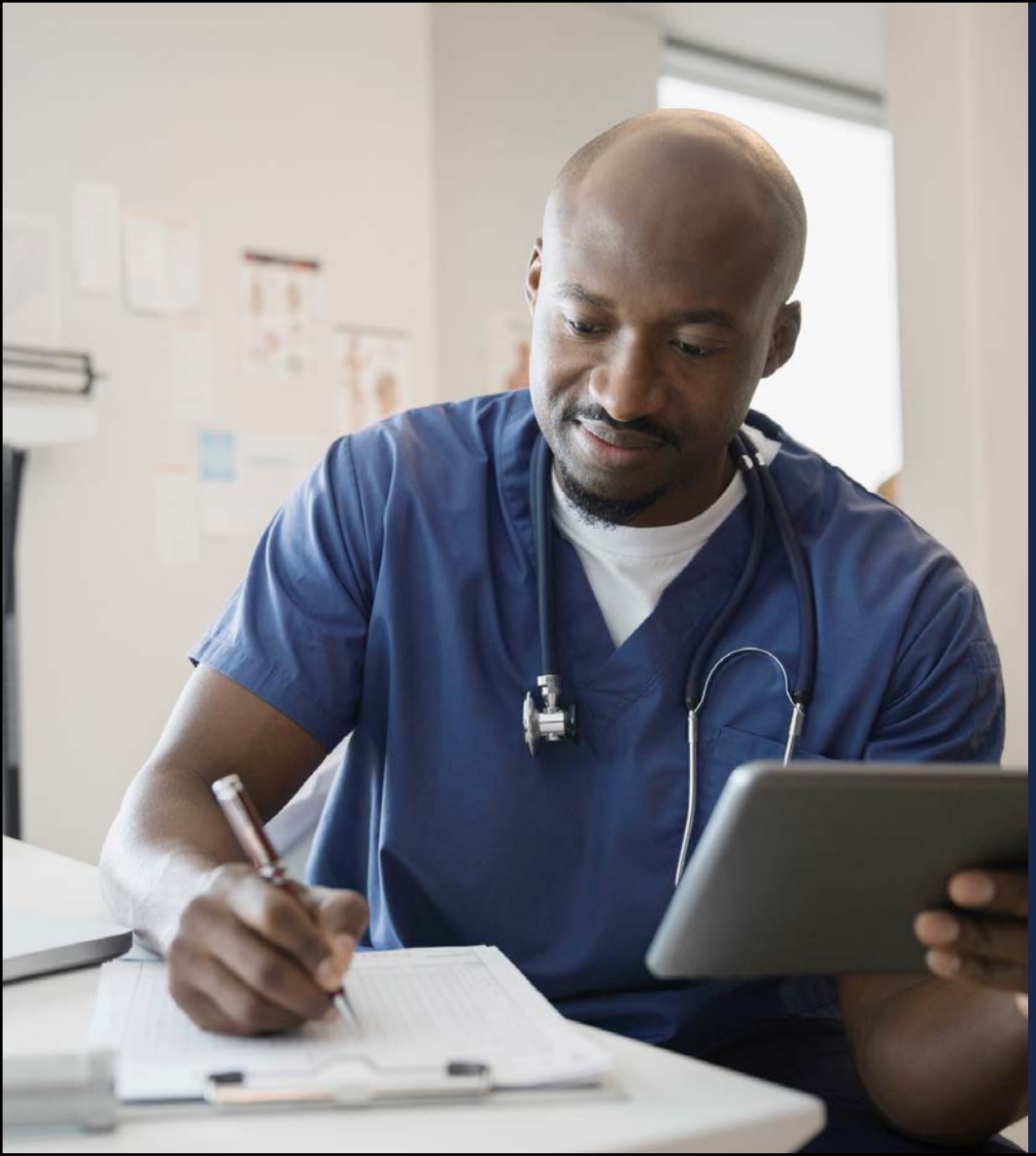
But :

- “May 25 is a starting point, not a deadline”
  - Industry peers have similar progress
- Many Data Protection Authorities struggle with resources

IMS Health & Quintiles are now

IQVIA™

Hubertus Stockmann



Mini Summit GDPR

Hubertus Stockmann

Regional Compliance Officer EMEA

Twelfth International Pharmaceutical and Medical Device Compliance Congress

14-16.05.2018, Vienna, Austria

The views and opinions expressed here reflect the my personal's and are not necessarily the views of Getinge.

GETINGE

We are Getinge

Key facts

1904
Founded in Getinge, Sweden

Carl Bennet
Entrepreneurial Chairman of the Board & Principal Owner

20
Production sites in 8 countries globally

+10,000
Employees worldwide

+150
Countries where our products are sold

22.5 BSEK
Net sales in 2017

2017 in numbers

Net sales: SEK 22.5 billion

Sales per region

- EMEA , 42%
- Americas, 40%
- APAC, 18%

Sales per business area

- Surgical Workflows, 35%
- Acute Care Therapies, 40%
- Patient & Post Acute Care, 25%

Sales per revenue type

- Capital Equipment, 48%
- Recurring Revenue, 52%

Our production sites

Americ
9 production sites
as

EMEA
15 production sites

APA
2 production sites
C

GDPR Readiness, in less than ¾ year…

Risk based approach to achieve GDPR Readiness

GETINGE

GDPR

High Level Process to achieve GDPR Readiness

Information Gathering

- Questionnaire
- Follow-up interviews

Gap & Risk Assessment

- Reports
- Recommendations

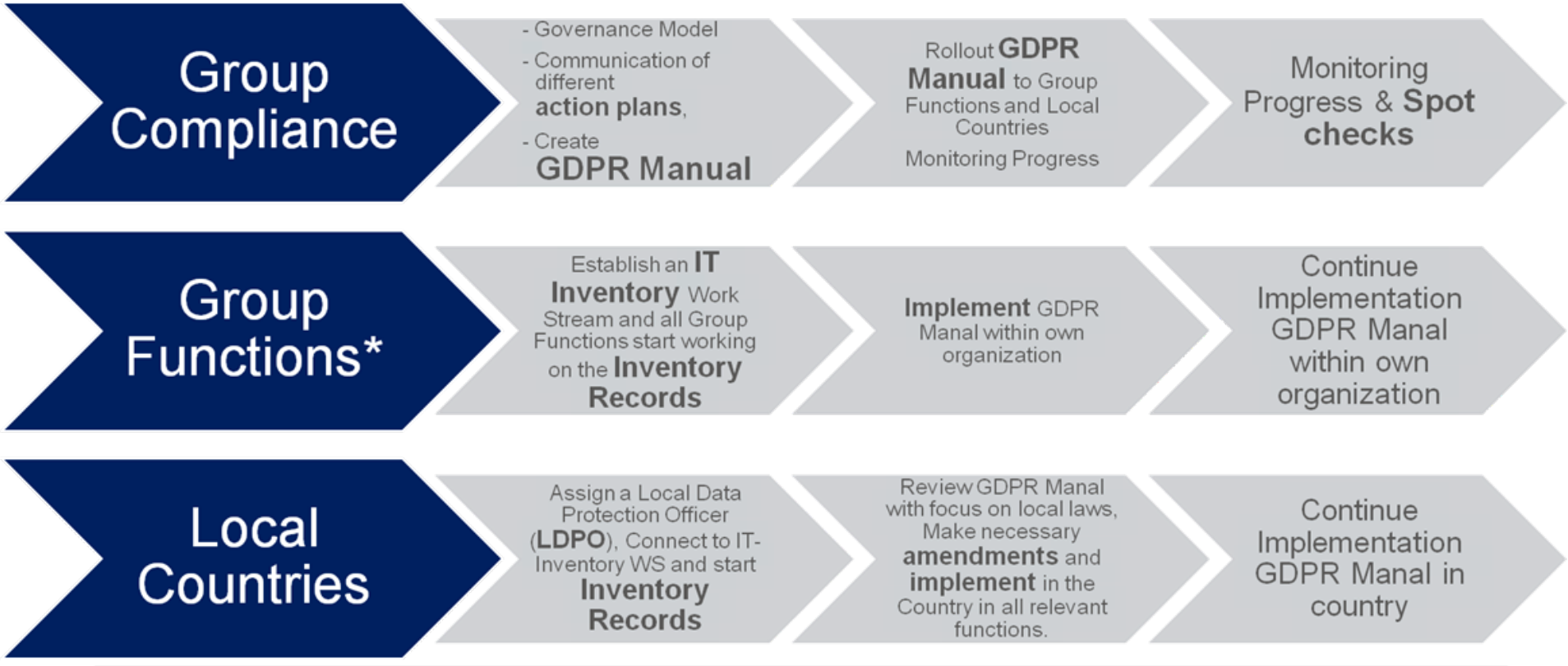
Implementation Plan

- Group Level action plan
- Country Level actions plan

GETINGE

GDPR

High Level Implementation Plan



* Communication & Brand Management, HR, IT, Purchasing, QRC, R&D, Sales, Finance

GDPR Challenges

Road blocks and other push backs

GETINGE

What the main Challenges?

Too much / few guidance

Most companies have sufficient policies in place.

Not knowing

Most people have an idea of what is right and what is wrong.

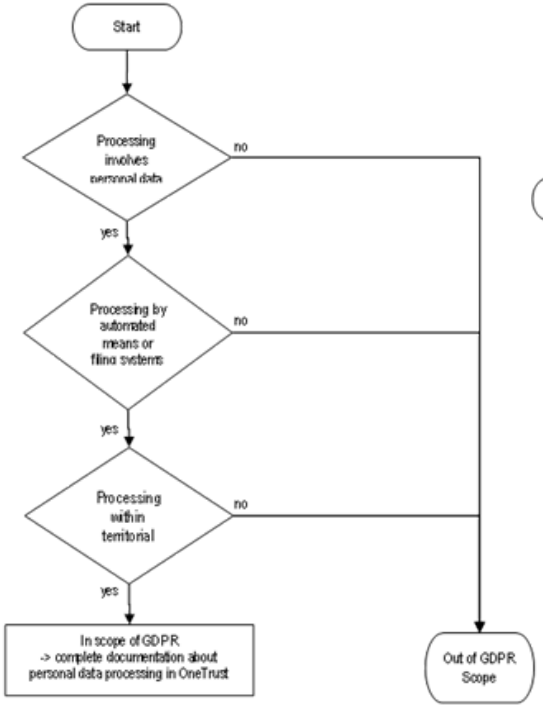
Ignorance

Some people think that willful blindness protects them.

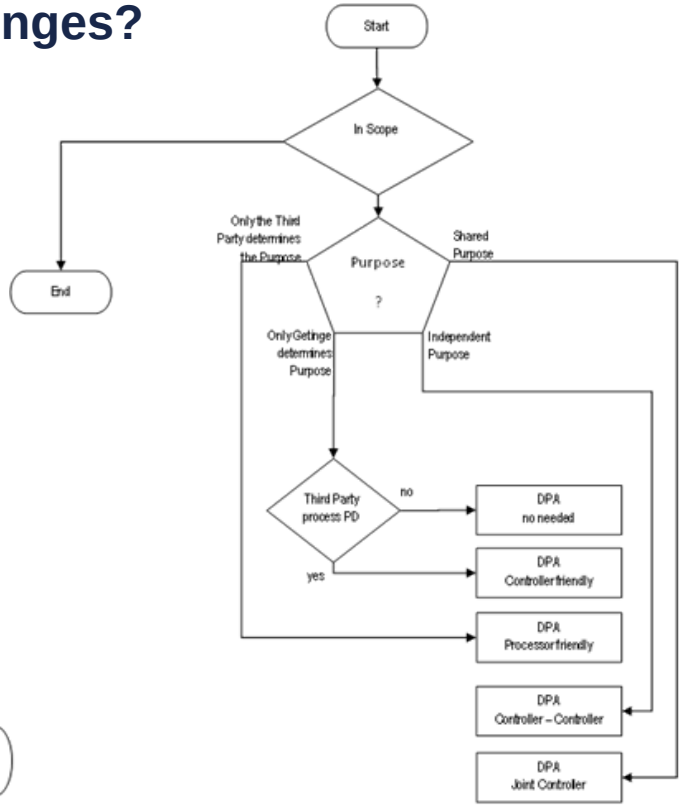
GDPR – What is coming next

Easy to understand implementation of various process flows

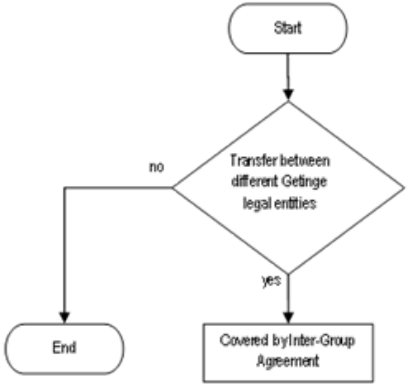
What the main Challenges?



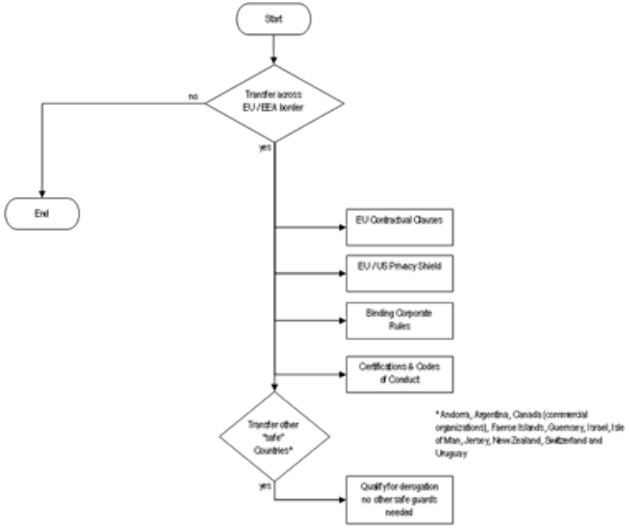
Determine Scope Process



External Contract Process



Internal Contract Process



Cross border transfer process

GETINGE

Thank you for your attention.

Any questions?

Hubertus Stockmann
+46 172 694 1966
Hubertus.Stockmann@geting.com

www.getinge.com

Getinge is a global provider of innovative solutions for operating rooms, intensive care units, sterilization departments and for life science companies and institutions. Based on our firsthand experience and close partnerships with clinical experts, healthcare professionals and medtech specialists, we are improving the everyday life for people - today and tomorrow.

GETINGE


GETINGE
PASSION FOR LIFE