GDPR

A Catalyst to Drive Real Action around Privacy and Security

Key factors for Boards and Executive Management to consider

Firms should not focus simply on deadlines, but on creating genuine long-term transformational dynamics

corix partners

WISE PARTNERS

nextworld CAPITAL

The General Data Protection Regulation

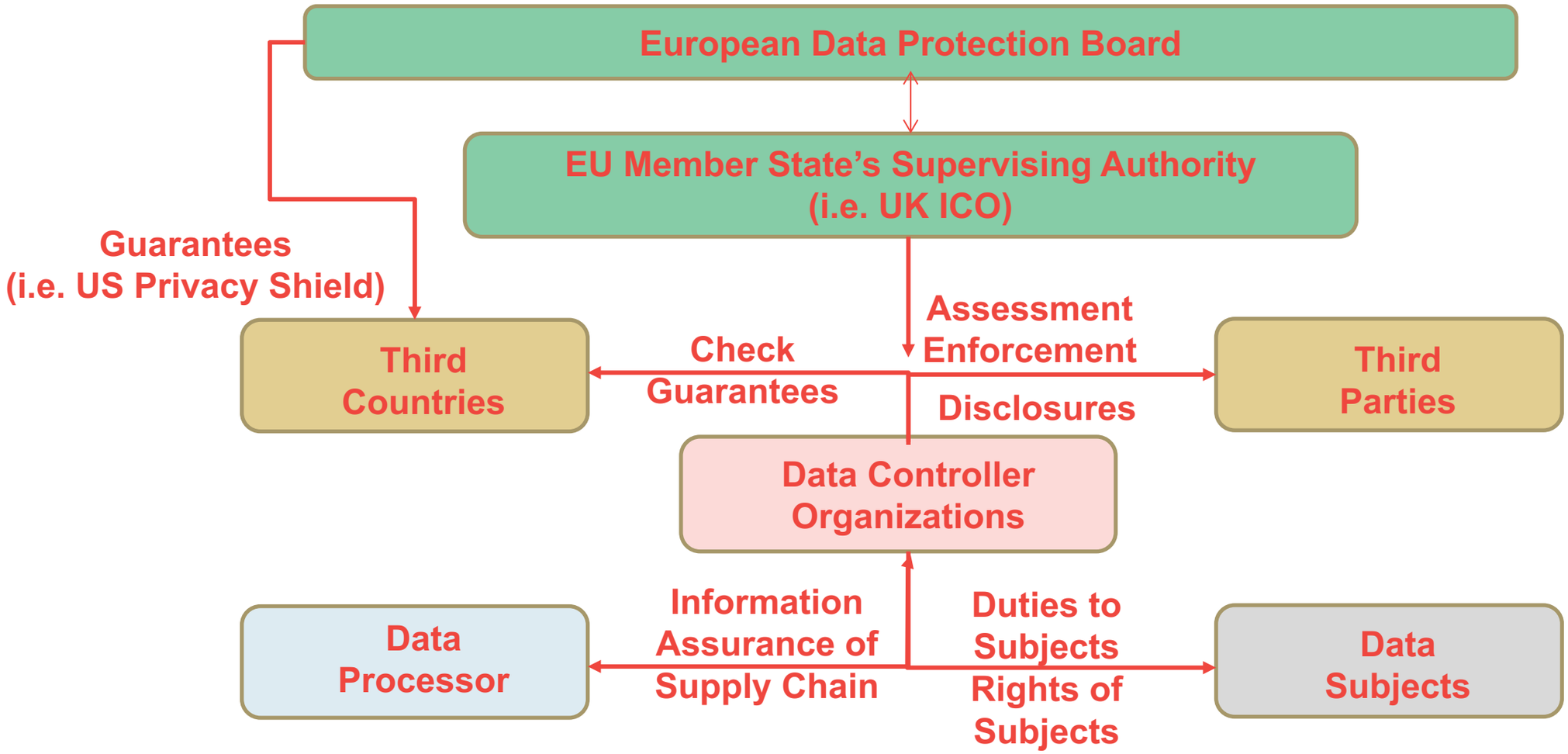
- It entered into force on 24 May 2016 and organisations were given 2 years to comply > It will apply fully from 25 May 2018

- It applies to all organisations controlling or processing data related to citizens of the EU member states, irrespective of geography

- Within the EU, it supersedes domestic legislation enacted as a result of the EU directive 96/46/EC
    - Although some member states may decide to enact specific domestic laws in support or ahead of the GDPR
- It introduces much stronger provisions, in particular around:
    - Role of the DPO
    - Data breach notifications
    - Consent and “Right to be forgotten” for the data subject
    - Penalties

The GDPR Governance Model

- **Most enforcement powers remain in the hand of the domestic data protection authority, under the supervision of a European Data Protection Board**



2 commonly held views about GDPR that have to be challenged upfront

GDPR and Brexit

Simply irrelevant ...

- UK firms controlling or processing personal data related to citizens of other EU member states will be expected to comply regardless (like US, Chinese or Brazilian firms for example)
- At time of writing, the UK is still expected to be a member of the EU on 25 May 2018
- In all cases, it is expected – at time of writing – that all pre-existing legislation and regulation would first transfer into UK law post Brexit before being re-examined if and when required
- The current UK government and the current UK ICO have indicated intention to enact or support similar legislation, even if there may be areas of conflict (e.g. between the GDPR and the UK Investigatory Powers Act) that might lead to legal or parliamentary scrutiny

2 commonly held views about GDPR that have to be challenged upfront

The 25 May 2018 Deadline

Relevant … but not so simple …

- This is not a “tick-in-the-box” exercise, to be completed by 25 May 2018
- This is about remaining in compliance thereafter, in a context where the legislation could well become tighter in the future or evolve country by country
- There may be an amount of cynicism amongst business communities around “yet another” piece of regulation, and some truly difficult aspects to enforce (e.g. the “right to be forgotten”), but it remains a genuine attempt to enhance privacy protection for citizens and consumers
- Where maturity is relatively high already around privacy and security, firms might just treat this an alignment exercise; but where maturity is low, it has to be seen as a fundamental transformational challenge
- If you are genuinely starting from scratch today, you have a problem that may take more than 12 months to fix …

What changes overnight on 25th May 2018?

Your Liability and Potential Fines

They can now reach up to EUR 20M or 4% of worldwide annual turnover (whichever is greater) for major breaches; EUR 10M or 2% of worldwide annual turnover (whichever is greater) for other breaches

- All obligations in the Regulation (many already existing in earlier legislation) acquire a different dimension under this new light
- HOWEVER …

1. The language used in the Regulation is far from being unambiguous, and there is no way of knowing how regulators will interpret it (e.g. “major breach”; “appropriate measures”), either on a case by case or country by country basis
2. Those interpretations may be inconsistent, and in turn be challenged in court
3. The actual level at which the first real fines will be set cannot be determined
    - Even if anecdotal evidence suggest that regulators have so far imposed heavy fines for major breaches in the context of their current limits and may continue to do so (e.g. the UK ICO imposed a fine of GBP 400k on TalkTalk out of a possible maximum of GBP 500k)

- IT WILL ONLY SETTLE THROUGH COURT CASES AND THIS WILL TAKE YEARS

1. Nobody wants to become a legal case, but it’s unavoidable that someone will be first …
2. Media interest could be high for brands which are already highly visible, potentially leading to reputational damage and loss of business
3. Group (Class) Actions could also emerge, with unquantifiable financial consequences if it leads to individual compensations

How to approach the problem?

- **What you need is a clear understanding of your current situation and a sound, realistic and actionable plan**

Think in terms of transformation and creating change dynamics (in particular if your starting point is low), more than raw compliance

- This is about becoming **and remaining** compliant over the years to come; not just putting a tick in a box on 25th May 2018
- For many organisations, most of this won't be new (e.g. the UK DPA has been in place since 1998)
- The GDPR introduces more stringent demands, but core principles remain the same and ask for data to be:
  - Processed lawfully, fairly and in a transparent manner.
  - Collected for specified, explicit and legitimate purposes.
  - Adequate, relevant and limited to what is necessary.
  - Accurate and, where necessary kept up to date.
  - Retained only for as long as necessary.
  - Processed in an appropriate manner to maintain security.
- You need to understand your real starting point, without assuming that this is a total greenfield for you, and without throwing resources upfront into the implementation of one-size-fits-all arbitrary checklists

Good cross-silos corporate governance is key to success

- **The fact that large corporates are heavily siloed and suffer from it when faced by complex problems is not new**
- **But GDPR compliance falls exactly in such category : This is not just a Legal problem, not just a Security problem, not just an IT problem …**

If maturity is low around data protection issues , identifying governance or cultural roadblocks that have prevented progress in the past is key to unlocking the transformational dynamics

- Appointing a DPO will be key if you don't already have one (assuming you need one – see GDPR art. 37)
- But the profile of the DPO is also essential
  - Must have gravitas and personal credibility to work cross-silos and be listened to
  - Must be independent of the Business and have direct access to the Board
  - Should typically sit within a Risk, Compliance or Governance function.
- The role is about orchestrating the delivery of a complex package of compliance measures
- Responsibilities and Accountabilities of all stakeholders have to be clear from the start

Ask yourself what could go wrong …

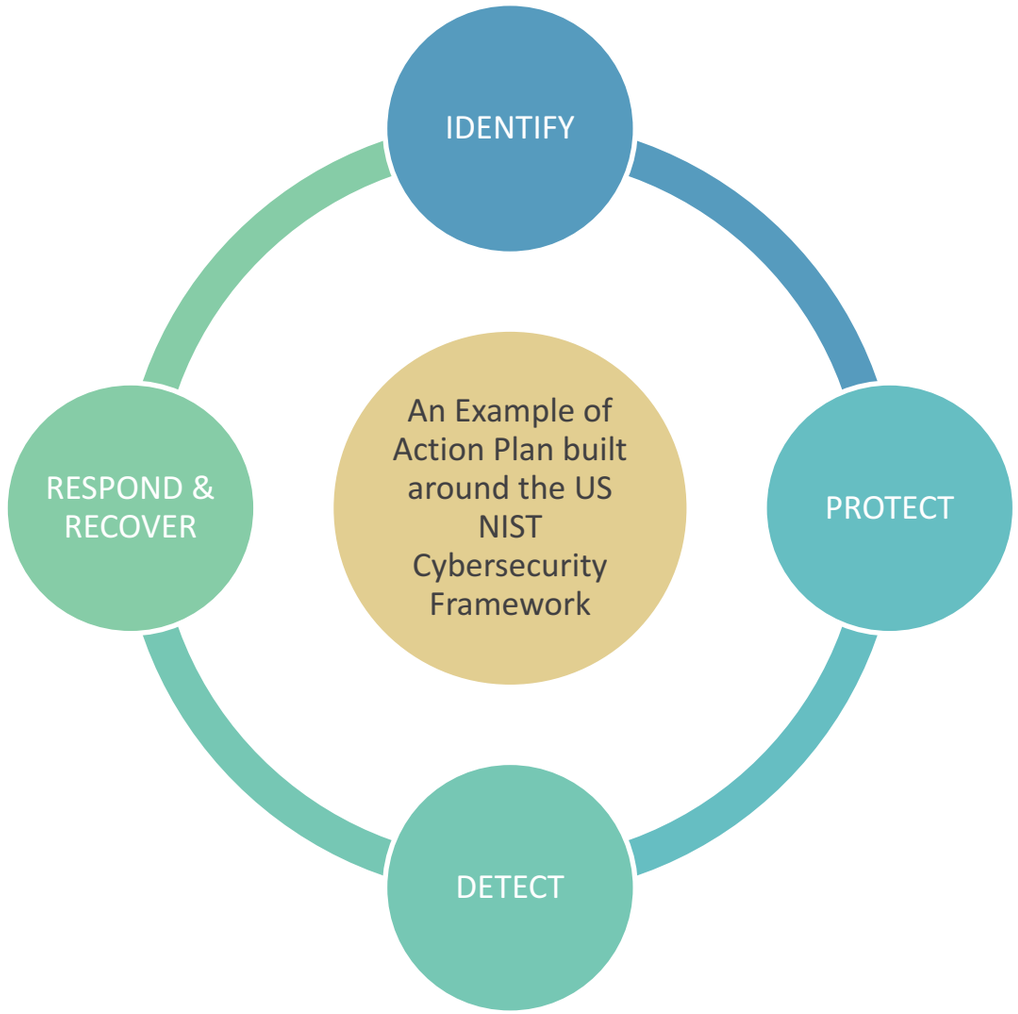
Look at the situation without complacency and build a plan

Do you know the personal data you hold?

- Who is processing it (internally and externally) ?
- Where does it flow to and from geographically ?
- How is processing covered ? In contracts ? Through Binding Corporate Rules ?
- How is consent obtained from the data subjects ?
- How is personal data identification and protection embedded within ongoing operational processes ?

How would you handle a data breach?

- Do you have a Data Breach Notification Procedure ?
- Do you have an Incident Response Plan ?
- Documented ? Regularly tested across all silos up to Board level ?



Do you have appropriate protective measures in place?

- Is sensitive personal data encrypted ?
- How are entitlements managed ? (including IT administrators, super users, generic accounts)
- What about data stored or processed in the Cloud and by other processors ?

Would you be able to report on a data breach to regulators within 72h?

- Are you logging and monitoring the right data internally ?
- Are you monitoring the Dark Web and Social Media for signs that may indicate a data breach affecting you ?
- Have you got the right people, processes and tools to analyse and report a suspected breach within 72h?
- What about data stored or processed in the Cloud and by other Processors?

Embed delivery of the action plan in the right Governance model

Board & Executive Management

DPO & Supporting Staff Functions (Risk, Audit Compliance, etc…)

All Stakeholders : IT, Security, Legal, HR etc…

The Role of the DPO

A complex and transversal role

Legal knowledge of data protection Regulation is not enough

- Must also have information security knowledge and skills
- An understanding of how to deliver data Confidentiality, Integrity and Availability measures within a management framework
- A good understanding of risk management and risk assessments
- Familiarity with and adherence to the codes of conduct relevant to the industry sector
- A good understanding of compliance standards and data marks
- A good understanding and a capacity to articulate “privacy by design” principles to delivery functions
- Able to coordinate and advise on data breaches and notification
- Able to make a cyber security incident response process work.
- Able to lead co-operation with supervisory authority
- Without any conflict of interest under relevant legislation and regulation

Single Person ?

Internal Figurehead supported the relevant experts ?

External team of experts ? (DPO-aaS)

Conclusions

- The GDPR is the strongest lever in years to drive real action around data privacy and security
- It brings a real risk of significant material impact on companies and their Boards of Directors

- But there is no magic technology solution
- Do not rush into appointing a DPO to shift the problem
- First, analyse your maturity posture with regards to data privacy and security
    - Quite a lot of this is not new and you should be already there on many points
- Where maturity is low, look back at the roadblocks that have prevented progress in the past, and build the right governance model to remove those
- THEN appoint the right DPO to assemble a clear action plan and drive it, so that you have a defendable position irrespective of your initial maturity posture

Evidence of real transformational dynamics and credibility of management backing are key for the short- to mid-term until the dust settles on all legal and regulatory matters

Contact

For further information please contact:

Jean-Christophe Gaillard / Neil Cordell
Corix Partners
+44 (0)7733 001 530 / +44 (0)7701 015 275
jcgaillard@corixpartners.com
neilcordell@corixpartners.com
www.corixpartners.com

Richard Preece
DA Resilience
+44 (0)7954 694 391
richard@daresilience.com
www.daresilience.com

David Hozé
Wise Partners
+33 (0)609 75 63 36
david.hoze@wise-partners.fr
www.wise-partners.fr

Frederic Halley
Next World Capital
+44 (0)7572 690 509
frederic@nextworldcap.com
www.nextworldcap.com

FINAL – 1.4 – March 2017

Many thanks to our focus group members, contributors & reviewers

Focus Group Members

Rupert Brown, Adelard LLP (Advisory CTO)
Stephen Deakin, Eccton
Bostjan Makarovic, Aphaia
Nick Simms, Cornwood
Johnny Stephens, SAGE
Peter Wenham. Trusted Management

Contributors & Reviewers

Maxime du Teil / Nicolas Bispo, ArsiaMons
Catherine Bouzigues / Pierre-Louis Couette, Wise Partners

Stuart Okin, 1E
Ray Stanton, Redwood Technologies