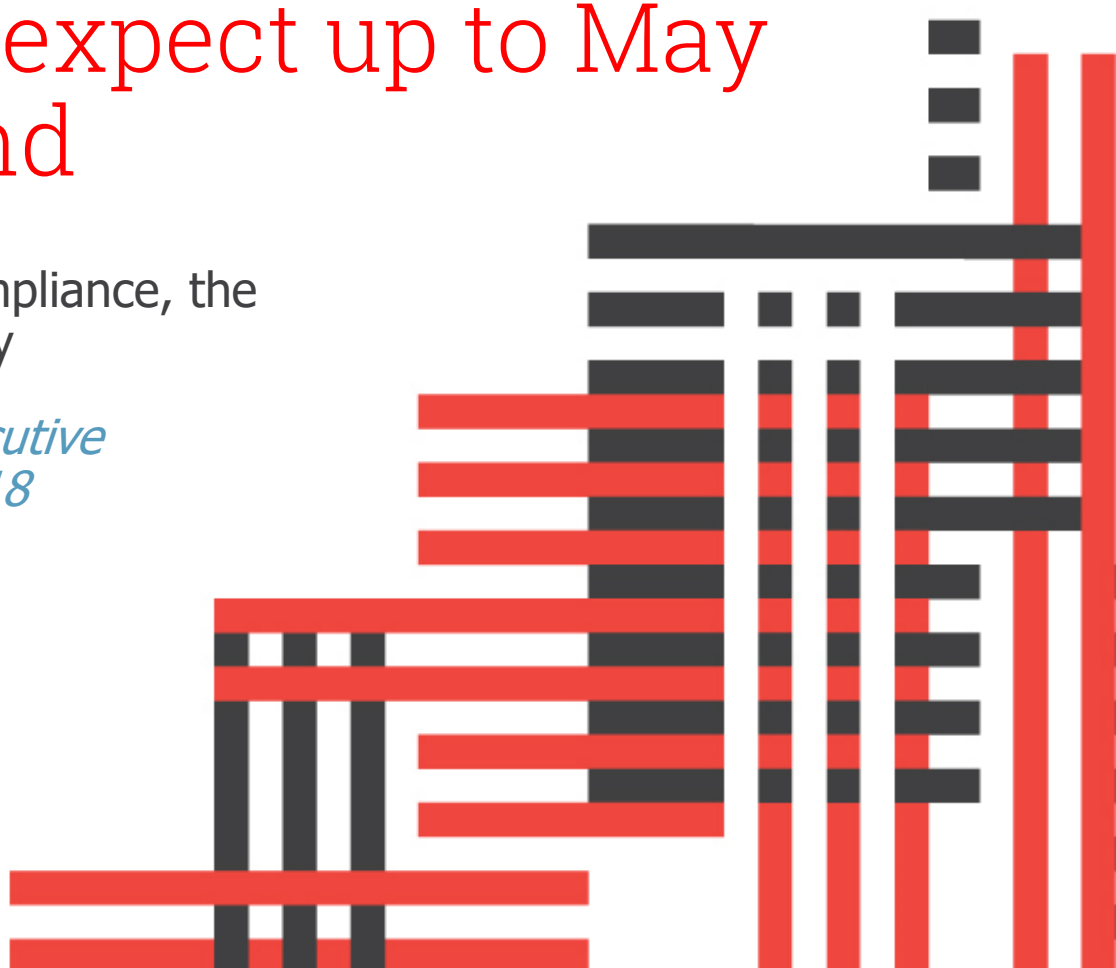
THE Security Transformation RESEARCH FOUNDATION

GDPR: What to expect up to May 25th and beyond

Faced with widespread non-compliance, the attitude of regulators will be key

Key factors for boards and executive management to consider in 2018

February 2018



GDPR: What's happened so far?

Throughout 2017, the GDPR has been successful in bringing up to the attention of boards, senior and middle management a range of security and privacy issues which had not been properly on their radar up to now

Many firms are currently involved in the delivery of large scale compliance programmes and have committed considerable amounts to GDPR (GBP 15M on average for FTSE100 organisations according to a survey by SIA Partners*)

GDPR has undoubtedly been a catalyst to engage with management layers which had been historically less involved with privacy and security matters, and to secure significant budgetary allocations in areas which had suffered from adverse prioritisation in the past

It has reached across industry sectors and across the economic spectrum, even if large B2C firms are obviously more concerned – and spending more on it – than smaller B2B organisations, and in spite of some sectors have been focused on other regulatory obligations in 2017 e.g. MiFID II in the financial industry

It is definitively perceived as forming part of a long-term social trend towards a more responsible and ethical use of personal data by corporate and public institutions

https://www.sia-partners.co.uk/preparing-gdpr-need-15m-300-450-per-employee-average-implement-gdpr/

The focus remains on “compliance”… but the concept is not well defined

”What good looks like” remains an elusive concept for many firms

The regulation is complex: 99 articles, literally hundreds of control points where “compliance” could be queried, and a language which remains open to interpretations in many areas: “Large scale”, “state of the art”, “adequate” protective measures, “undue delays” in reporting etc …

“Compliance” is not a fully defined concept and firms are having to determine for themselves “what good looks like”, often with the help of third-parties (and “snake oil” vendors also proliferate as a result…)

Faced by what is essentially a transversal problem, each corporate silo tends to focus “compliance” and their priorities on what they understand best and what is closest to them

Generally, the issues are often framed around “data”, more than the associated processing activities, their nature, legitimacy or sensitivity

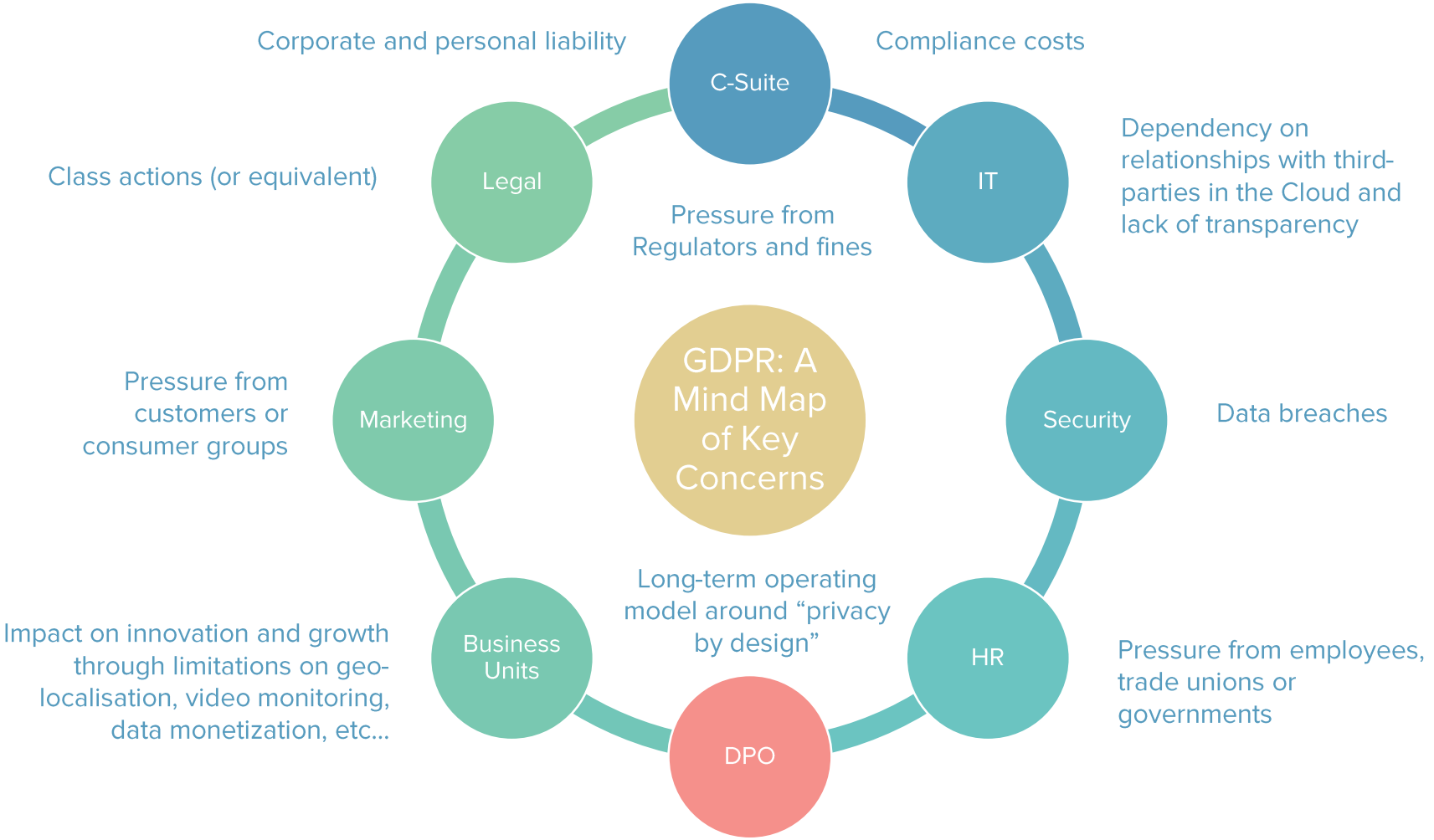
The role of the DPO is in the process of establishing itself, but its imposed independence makes it difficult to position and to operate for many firms

Many voices are emerging – in particular in the B2B sector – around the actual need to appoint a DPO versus a “Chief Privacy Officer” type of role, which could be less constrained and more hands-on

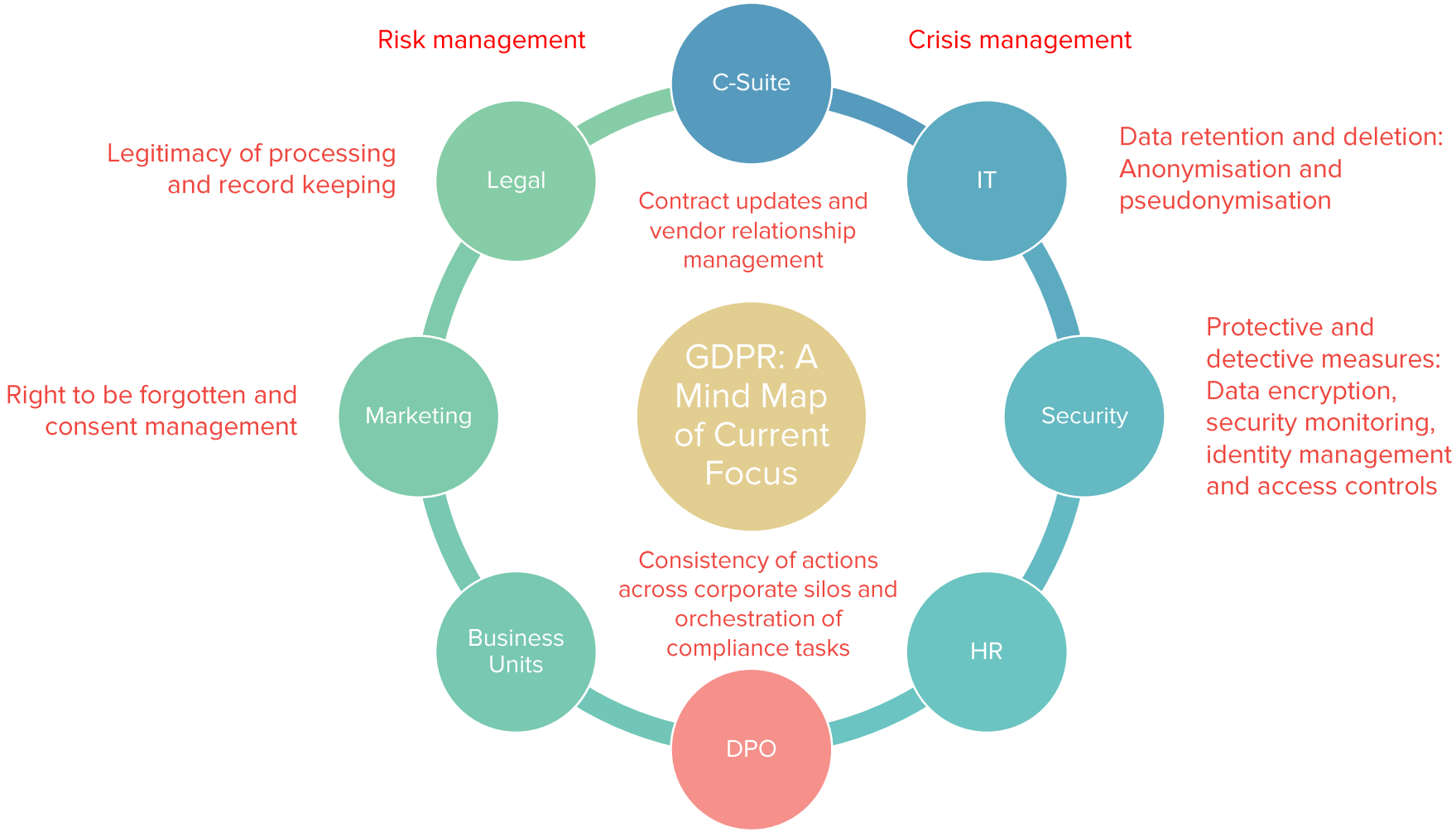
The outlook the regulators will take in the end is unknown, and the official guidance produced so far has only shed limited light on those matters in practical terms

Over time, “compliance” labels may emerge but they will need to build credibility and will face the same range of issues around definitions to start with

GDPR: A Mind Map of Key Concerns



GDPR: A Mind Map of Current Focus

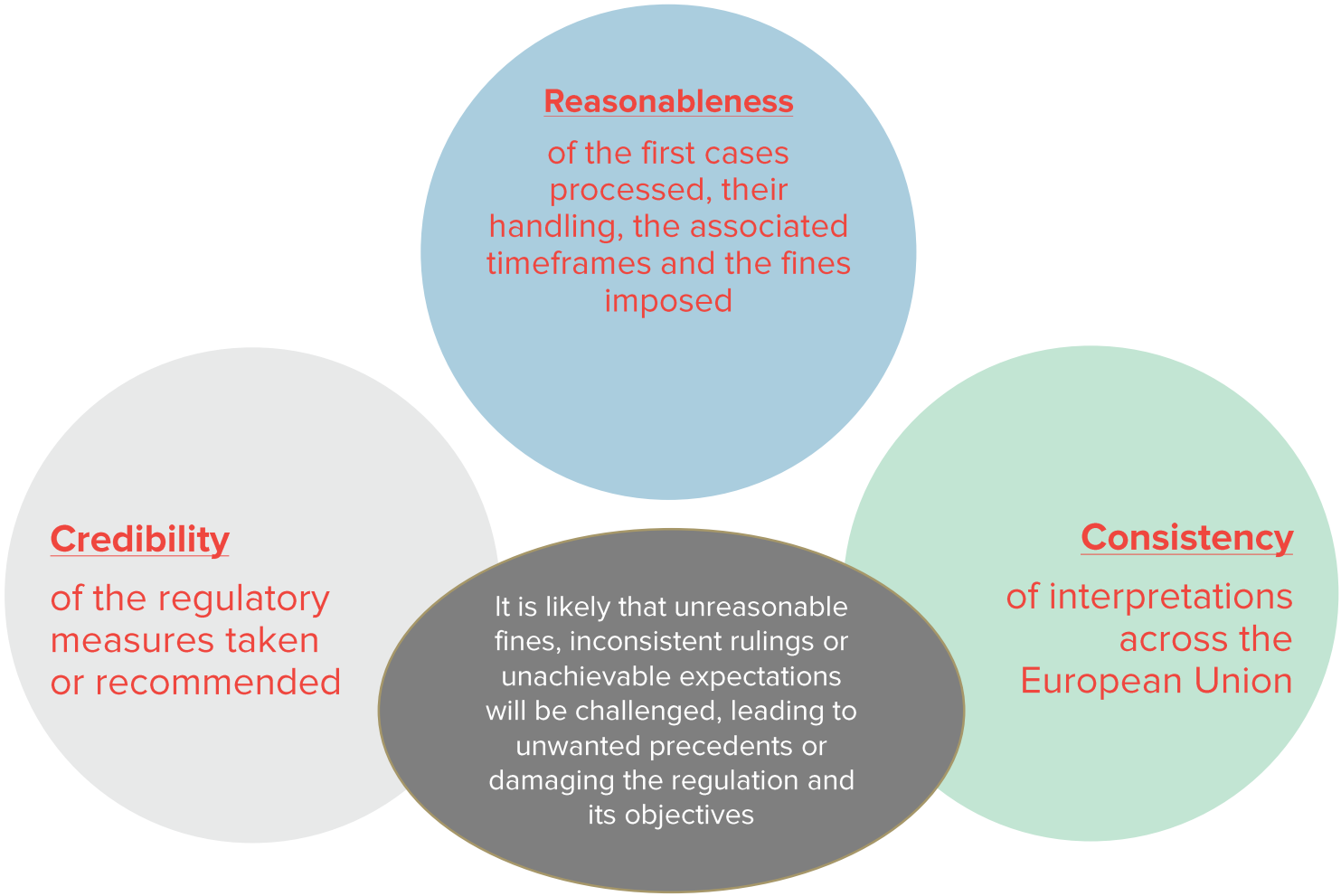


GDPR: The "known unknowns"

Nobody really wants to be first organisation processed under the GDPR but it is unavoidable that someone somewhere will be first

- Which country will be the first to act? Is it conceivable that some regulators could start "knocking on doors" on May 28th?
- Should multinational firms be concerned about a risk of contagion (one investigation in one country leading to other regulators opening a case)?
- Is it conceivable that some regulators could take a much harder – or more lenient – line than others forcing precedents across Europe?
- What will be the profiles of the first cases processed under the GDPR? At which level will the first real fines be set? Will they be challenged and in front of which court? On what grounds? Would these challenges be successful?
- Could there be any conflict with other regulations (e.g. ePrivacy) or domestic legislations?
- What will be the real investigatory capability of the regulators and will they be able to focus on more than just high profile cases? And could it be that nothing really happens for most firms across the continent after all?
- Is it conceivable that the GDPR could be just a huge sledgehammer aimed at major US tech firms (Google, Facebook, Uber etc…) or Chinese/Russians interests? What will be the true independence of regulators across the EU from political or economic actors?

The regulators have a very fine balance to find (collectively)



The attitude the regulators will take: The key factor from now on

The attitude the regulators will take post May 25th in enforcing the GDPR is now the key factor for the year ahead but cannot be predicted

- 80% of firms will not be "compliant" (whatever that means)
- 50% of those would have made a deliberate choice on the matter after weighting costs and risks

(Source: Forrester – Predictions 2018 "A Year of Reckoning")

Privacy regulators across the EU have been asking for more powers for a decade so it must be expected that they will seek to exercise those as the GDPR comes into force post May 25th

But each domestic regulator has its own legacy practice, its own concerns, constraints, resources, priorities; those factors will not vanish overnight and will continue to influence the way the GDPR is enforced

Beyond May 25th, the key milestone ahead is now the unknown point in time (post May 25th) when the first regulatory ruling under the GDPR will be published

The Role of the DPO will become pivotal in large firms but the DPO cannot act alone

It is a cornerstone of the new regulation but, beyond its imposed independence, it must establish itself as an effective and efficient corporate function

In practice, it is a new industry emerging across Europe with 28,000 roles expected to be created (Source: IAPP*) but it will take years for the relevant education and certification programmes to be fully each established in all countries

The role must be independent from processing, but many stakeholders still expect practical guidance from the DPO on how to interpret the regulation and implement compliance; it must not become a useless "ivory tower" role

Orchestrating compliance across corporate silos in large firms will make the role a senior and complex transversal leadership role, which must attract an executive with a deep knowledge of the internal workings of the firm

Beyond the actual role, there is a set of very diverse competencies associated with the function (legal, technical, etc…) which could be spread across a team – internally or externally

https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/

Beyond arbitrary independence principles, how will the DPO work in practice?

A clear operating model is essential to define all roles and responsibilities around the DPO function

Operational teams rightly demand clarity and consistency on what is expected from them around GDPR pre & post May 25th

"Compliance" – once defined – must not be seen as a static concept; it will evolve post May 25th as rulings and precedents emerge

Who becomes responsible for interpreting the regulation and its forthcoming evolutions, and giving practical guidance to operational teams on building and maintaining compliance?

If it cannot be the DPO on grounds of independence, positioning and structuring this competence clearly and practically in the organisation is key

What to do next?

If you already have a compliance programme underway

Do not obsess over the May 25th deadline, look without complacency at roadblocks and priorities, and keep going

- This is not a "box-ticking" exercise and nothing stops on May 25th; keep the dynamics going and set realistic and achievable management expectations and compliance timeframes

Evidence of strong management backing and a genuinely trackable long-term approach towards putting in place the "privacy by design" principles which are at the heart of the regulation, should always play in your favour with regulators, irrespective of the actual compliance challenges you may be facing.

- The objective must be to remain in compliance once the current programme of work has delivered on its objectives
- Expect that perceptions and priorities will change with stakeholders during the second half of 2018 as soon as regulators start taking action and precedents emerge
- The DPO will have as a key role to play in orchestrating this phase in many firms; if not in place, the role – or some equivalent leadership function – must be assigned ASAP
- More than ever, strong transversal governance is paramount; start looking across corporate silos towards an effective and efficient long-term operating model around the DPO role to ensure ongoing "privacy by design"

What to do next?

If you are really starting now

Appoint a high-profile Data Protection Lead immediately and build a plan looking towards May 25th and beyond

- Do not rush into buying any alleged technology solution to a problem you don't understand properly
- Focus the pre May 25th window on analysing your potential level of exposure and launch immediately a set of practical tasks which will force stakeholders to confront the topic ahead of May 25th
    1. Start building a registry of your processing activities (nature, type, legitimacy, sensitivity, cross-border transfers, processing arrangements with third-parties etc..); assess the real volume of personal data you hold
    2. Engage with all relevant stakeholders around the long-term role of the DPO, whether you need one, who that could be, and where the role could fit in your organisation; consider whether the appointed Data Protection Lead should become DPO in the run up to May 25th
    3. Review Privacy Notices on websites and in employee charters / codes of conduct, Data Subject Access Requests and Data Breach / Crisis Management procedures; if those don't exist, create them immediately involving all stakeholders; otherwise, bring them in line with GDPR expectations
    4. Organise a scenario-based data breach test involving all stakeholders across the firm up to Board level (IT, Legal, HR, etc…)
    5. Keep a track record of each decision taken and why
- In parallel, identify realistic year-end compliance objectives, build a plan, a delivery team and a budget

Contact Details and Acknowledgements

Pierre Poinsignon
Arsia Mons
pierre.poinsignon@arsiamons.fr
+33 (0)6 15 45 85 68
www.arsiamons.fr

Jean-Christophe Gaillard
Corix Partners
jcgaillard@corixpartners.com
+44 (0)7733 001 530
www.corixpartners.com

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

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

David Hozé
Wise Partners
david.hoze@wise-partners.fr
+33 (0)6 09 75 63 36
www.wise-partners.fr

Many thanks to our focus group members, contributors and reviewers

Mark Segelov, Colt Technology Services
Nick Simms, Cornwood Risk Management
Rupert Brown, The Cyber Consultants
Ross Jackson / Harvey Seale, Mimecast
Andrew Bullivant / Alistair Roberts, Pension Insurance Corp.
Karin Lange / Jean-Marie Lapeyre, PSA Opel Vauxhall
Steve Lamb, Rapid 7
Neil Cordell, Target Group

Laure Jallet / Cecile Lagardere, Care Insight
Yann-Herve Beulze, Groupama Asset Management
Catherine Bouzigues, Wise Partners

THE
Security
Transformation
RESEARCH FOUNDATION

www.securitytransformation.com

@Transform_Sec

The Security Transformation Research Foundation is a dedicated think-tank and research body aimed at approaching Security problems differently and producing innovative and challenging research ideas in the Security, Business Protection, Risk and Controls space

FINAL – 1.0 – February 2018