Privacy Culture

Demonstrating compliance by keeping records

Steve Wright
Data Protection Officer

8 May 2019

Agenda for today

1. Introduction to Privacy Culture
2. Demonstrating compliance with Article 30
3. Building a 'Defensible Position'
4. Operationalising Privacy 'Target Operating Model'
5. Enhance your Training, Awareness and Communications
6. Demonstrate Accountability

Introduction to Privacy Culture

Vickie Guilloit, Steve Wright & Partners

Together we have 40+ years of unparalleled experience in the fields of data security, data privacy, and culture change including programme management and digital transformation.

Bringing genuine real-world experience to deliver pragmatic privacy, data security and cultural change programmes.

Helping clients create ‘good enough’ GDPR frameworks, and helping to operationalise privacy and security processes, policies and measurable controls.

We also help organisations to feel inspired, motivated and equipped to do the right thing, regardless of the size and shape of your organisation.

~ GDPR Maturity Assessment (1 day)
~ Benchmarking – Industry comparison
~ Coaching, advisory and projects (DPIAs)
~ Tools and efficiency accelerators
~ Risk workshops / Ops improvement
~ Target Operation Modelling
~ Interim DPO & CISO
~ Training, awareness & eLearning
~ Educate and embed Privacy & Security

Steve.Wright@PrivacyCulture.com

Demonstrating compliance with Article 30

Under Article 30 –Record of Processing Activities, you should be able to demonstrate:

- Records of processing activities – explaining the purpose
- Any special categories of personal data
- Document the legitimate interest assessment has been completed
- Erasure and deletion regimes
- Link to relevant security policies and procedures
- Detail if third party data processors or third countries and what provisions
- How transparency and accountability is being achieved

- This links to your overarching ability to be in a ‘Defensible Position’…

Steve.Wright@PrivacyCulture.com

Defensible position

utilising the GDPR Maturity Framework™

Irrespective of how compliant or careful you are to comply with GDPR requirements, inevitably you may face some level of enforcement action against you. This could be class action from a disgruntled employee or customer, or, it could be brought against you for failure to act in a way deemed necessary by a regulator. Either way, a strong defensible position should help thwart or reduce the level fines / compensation you may be liable for under GDPR. So, your ability to defend yourself should focus on three key components, each made up of sub components.

3.0 1. Accountability
Defined and understood, Data Governance, determined with RACI & DPO appointed. Appropriate ownership and that responsibilities are known and understood at all the staff levels. A5

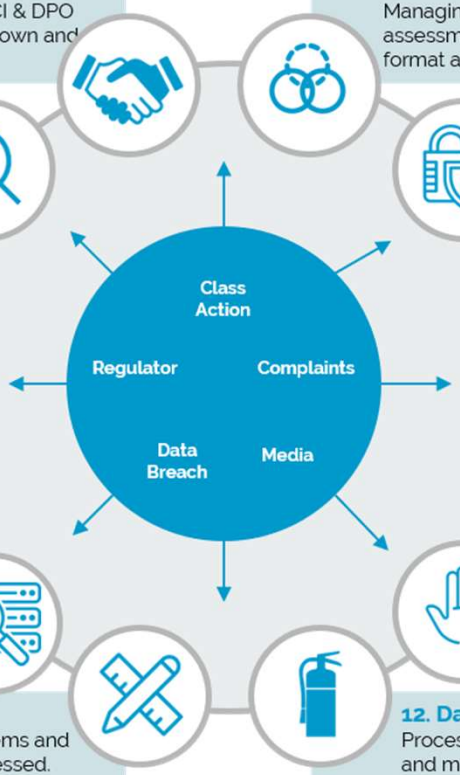
2.5 2. Lawfulness, Purpose limitation, Accuracy
Data processing meets the legislative of being processed lawfully, Including: 'purpose limitation', 'data minimisation', and 'accuracy'. A5, 1(b-d), A6- 10

3.0 3. Retention & Deletion
Personal data is processed for no longer than is necessary for the purposes for which it was collected & Deletion procedures in place. A5, 1(e,

2.0 4. Transparency
Current, accurate, relevant and communicated privacy and/or cookie notices for all business processes. A5, 1a - transparency, A12 -14,

3.5 5. Records of Processing Activities
The Record of Processing Activities complies with GDPR regulations, and is comprehensive, accurate, current and accessible (describes the purpose). A30, A5 (2)

3.5 6. Data Protection by Design & Impact Assessment
Data Protection by Design and Default is embedded into all systems and process/business changes, or where ever personal data is processed. Articles 25 and 35 + Article 29 WP - Guidelines on DPIA



7. Risk Management & Control Framework 2.0
Managing privacy risk including defining risk appetite, conducting risk assessments, methodology, recording and reporting risks in a standard format and treatment of the risks identified..

8. Data Security 3.5
Implemented appropriate technical and organisational security measures to protect data subjects' fundamental rights and freedoms. A5 (1f), A32

9. Policies, training, awareness, culture 2.0
Data protection policies/procedures in place and staff adequately trained. Awareness and culture change programme. A24

10. Third Party Data Processors 2.5
Appropriate contracts in place with data processors; processors have provided sufficient guarantees. A28 and A29

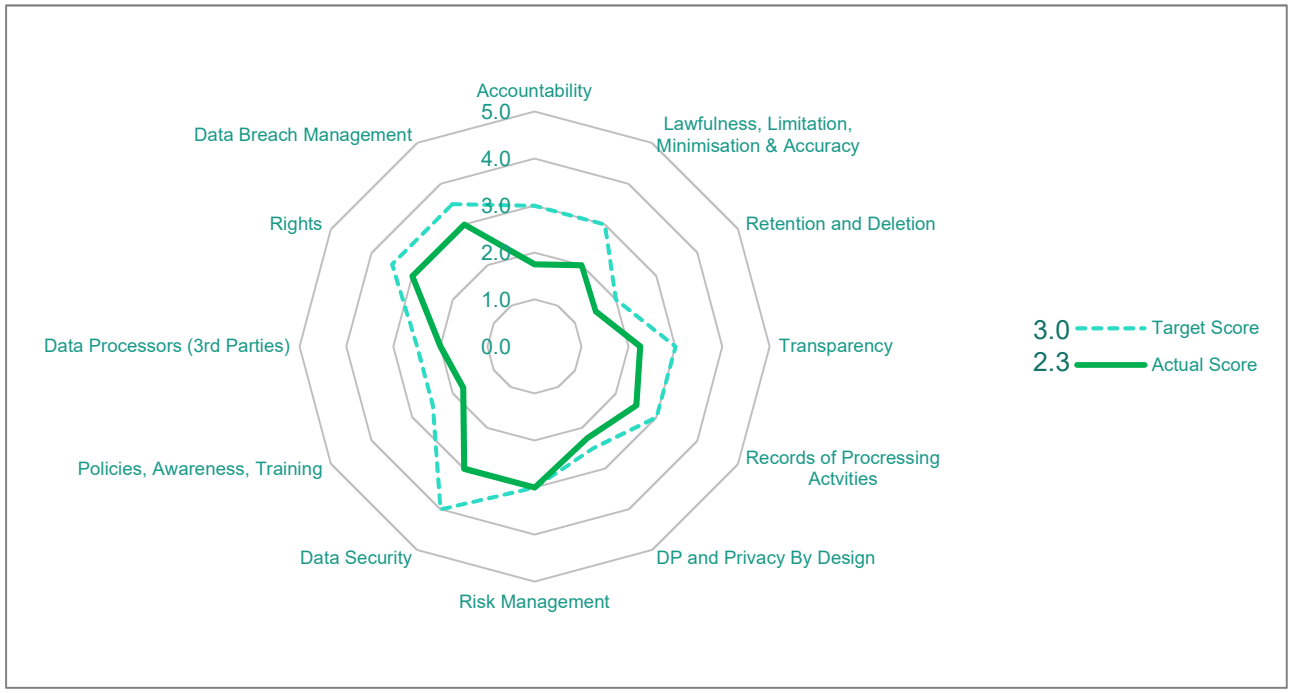
11. Data Subject Rights 3.0
Data subject rights catered for either manually or automatically. Supported by processes and procedure put in place to manage. A15 to 23, 34

12. Data Breach & Incident Management 2.0
Process updated to cater for 72 hours notification Processes to detect and manage personal data incidents - including process to report to the ICO or individuals..Procedure must be tested & rehearsed, A33-34

Steve.Wright@PrivacyCulture.com

Measuring your level of GDPR Maturity (example)

Using the Defensible Position and by utilising the GDPR Maturity Framework , the following subjective findings summary scores were applied across each of the twelve domains.



From the analysis conducted, your organisation are showing slightly below average score, but these are all subjective and not means tested. It does however highlight some of the areas the need further focus, including:

- Simplified privacy workbook and end user designed compliance documentation
- Process simplification for business PIA & Privacy by Design integration
- Training, awareness and communication roll-out, train the trainer
- Information Governance, RACI and self-attestation compliance framework
- Privacy Control Framework – used to sync with security compliance and 3rd line testing

Key:

Optimal and independently verified = 5
Managed controls and benchmarked = 4
Managed controls but not benchmarked = 3.5
Defined controls and fully implemented = 3
Defined but not fully rolled-out = 2.5
Repeatable controls = 2
Ad hoc but some controls = 1.5
Initial but ad hoc = 1
Non existent = 0

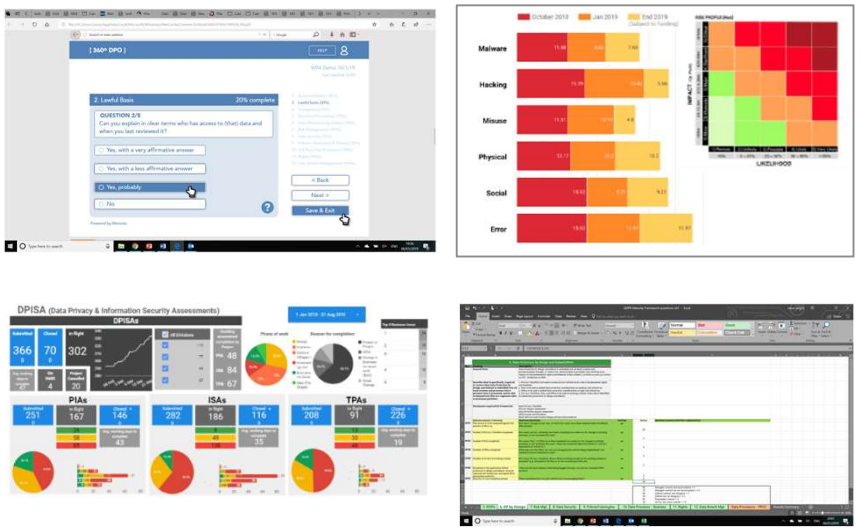
The GDPR Maturity Framework is a set of GDPR questions, split across 12 domains that have been developed utilising the UK regulator's ICO checklist, including Article 29 Working Party guidance, and EU EDPB guidance, and all of the GDPR Articles and Recitals. It is a practical interpretation of the GDPR text that takes into account the 'how' and 'why' a particular implementation or risk mitigation was selected. It is not an audit framework, as the questions were developed in a way that would encourage the interviewee to be open and transparent in respect to their level of understanding, knowledge and accountability and does not rely on substantive evidence. The maturity scoring (0-5) is also subjective and is based on the responses to the questions. It is however, a very good indicator as to how mature the procedures, documentation are that an organisation has in place, and can be used as a measure of GDPR maturity or how well an organisation has 'operationalised' its GDPR practices. The maturity rating has been developed using the internationally recognised Capability Maturity Matrix Integration (CMMI) developed by Carnegie Mellon University.

Steve.Wright@PrivacyCulture.com

Understanding your level of GDPR Maturity

- The benchmarking incorporates 12 common privacy themes to measure and compare organisations against, and benchmarked scores across each area, using data collected across 30 differing business.
- The maturity rating was developed using the internationally recognised Capability Maturity Matrix Integration (CMMI) by Carnegie Mellon University.
- The results will feed into a overarching GDPR Benchmarking Report that will determine how mature the organisation is (in terms of GDPR adoption).
- You can use it to validate your level of GDPR maturity, identify areas of improvement and will help you make appropriate recommendations.
- This will also help you understand your level of risk exposure, so you can prioritise scarce resources and budget.
- This will help you areas where further efficiency could be achieved, and ultimately help you set a course of direction for 2019 and beyond.

Figure 1. GDPR benchmarking tool (on line)

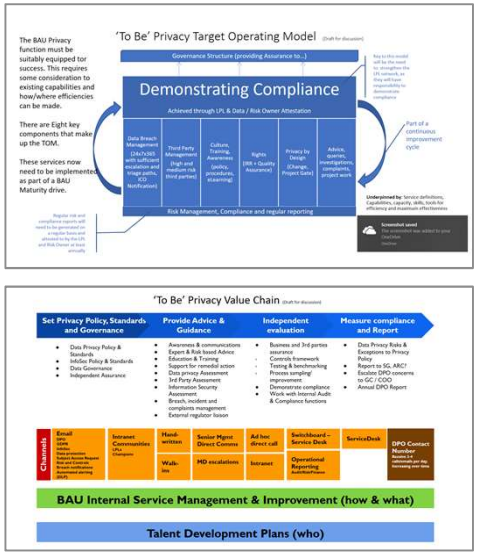


Steve.Wright@PrivacyCulture.com

Operationalising Privacy 'Target Operating Model'

- Using existing documentation including the benchmarking data, you can design and build your organisation a Target Operating Model – TOM (See Figure 2).
- Ensure that this model is fit for purpose and future proof. You can accelerate this process by utilising previous models, building upon successful existing practices. This can be achieved through workshops, interviews, and engagement of key stakeholders.
- No one size fits all, but there are some fundamental service components and capabilities that every privacy function should be operating with.
- Many DPO's are struggling to identify how such functionality can be achieved and how to operationalise, build, improve, or embed these services.
- This is not uncommon given the relatively new areas of GDPR. Areas where common immaturity exists include: PIA process (often clunky and labour intensive), DSR processes (gaps in process), and how to make a lasting GDPR change to the culture of an organisation.
- You need to produce a model with service definitions, calculation of time and effort to help determine headcount, and will provide service level agreements and set targets for reporting via KPIs.

Figure 2. Target Operating Model

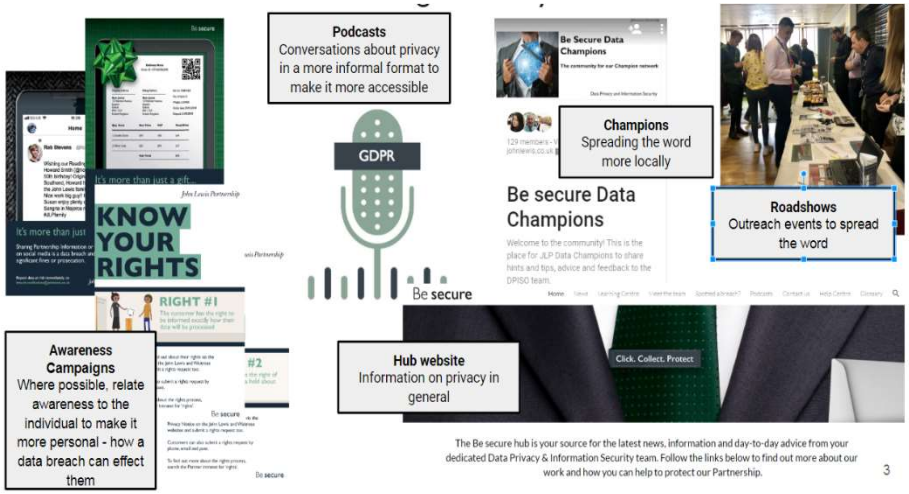


Steve.Wright@PrivacyCulture.com

Enhance your training, awareness and comms

- The challenge is how to convince business employees and senior leadership to engage in GDPR, and ensure that appropriate privacy and security behaviour is integrated into their day to day responsibilities.
- Figure 3.0 includes some examples of how we can avoid being boring, or not relevant to audiences.
- A suggested approach would be to utilise the findings from the Benchmarking, together with feedback from your organisation employees.
- Work out the most effective communication channels to reach a specific audience, and which processes or cultural issues are currently preventing employees from adopting the expected behaviours.
- Ensure that the impact of the change on employees is assessed before any programme of awareness, education, and training is introduced.

Figure 3. Training, communication & Culture Change

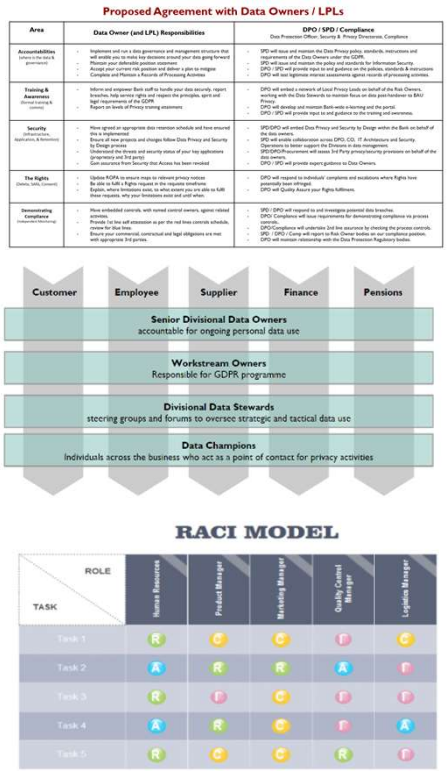


Steve.Wright@PrivacyCulture.com

Demonstrate Accountability

- Accountability is key to demonstrating compliance with GDPR. However, in large complex organisations this takes significant work and commitment, as each department or business will have different data needs.
- You will need to have differing ideas about what ‘good enough’ compliance looks like, and how Governance should operate and work across the business.
- Help your organisation to articulate where each business unit or department should be in terms of GDPR compliance and will create the right Accountability and Governance structure to ensure compliance can be maintained.
- Demonstrating Accountability can also help focus thinking and how to manage data privacy and data protection at the business level.
- Try to leveraging existing Governance structures, RACI matrices, hierarchy and roles to ensure the right framework exists, or coexists within existing organisational structures.
- It is important to focus on building the right structure where it matters, where resources and budgets are constrained, the key to longevity is ensuring the right repeatable framework is in place and operational.

Figure 4. Demonstrating Accountability



Steve.Wright@PrivacyCulture.com

Top five tips

1. Build a comprehensive ROPA (Article 30)
2. Build a 'Defensible Position'
3. Focus on operationalising privacy (Target Operating Model)
4. Change the culture (by enhancing your Training and Awareness)
5. Demonstrate Accountability

Steve.Wright@PrivacyCulture.com

Thank you

Steve.Wright@PrivacyCulture.com

Tel: 00 44 (0) 7771 301 372