www.pwc.co.uk

General Data Protection Regulation Readiness Assessment Tool

February 2018

pwc

The GDPR Readiness Assessment Tool (the R.A.T.)

Targeted assessment of compliance gaps to prioritise remediation activities required

The R.A.T. is an 'Intelligent Questionnaire' which asks a series of 72 questions in a two-hour workshop to assess your current state of data privacy and your readiness for the GDPR.

PwC's maturity matrix is built upon two pillars, 'Privacy Architecture' and 'Privacy Principles'.

The set of questions have been developed to align with the criteria in the two pillars. Respondents select from four predefined answers. This ensures that data are comparable across business functions and territories and over time, as the R.A.T. is designed to be repeatable.

The questions are linked to every Article and Recital of the GDPR and can be mapped to:

- Regulatory Risk issues
- Decisions in court cases
- Causes of consumer complaints
- Our Enforcement Tracker

The R.A.T. contains demographics questions, so you can benchmark against others.

Result:

A comprehensive tailored report which provides you with full visibility of your GDPR Readiness, reveals gaps in your compliance and provides a risk-based approach for prioritising your compliance work.

Assessment approach

What we need from you:

120 mins (approx.)

With the following people:

1. Data protection officer
2. Information security
3. Information governance
4. Risk and compliance professionals
5. Legal practitioners

To provide us with the information we need about your:

Data protection architecture

Compliance with the GDPR principles

Our methodology

Privacy transformation Step 1 – Assess | **Step 2 – Measure**

R.A.T. | **Special characteristics workshop** | **Gap analysis**

Use the Readiness Assessment Tool to assess current compliance maturity

Facilitated Workshop to understand 'Special Characteristics'. Utilising also the R.A.T. results, we help you to define the program vision and to understand critical embedded legacy risks

A Gap Analysis to identify at a granular level, the incremental work that needs to be done to achieve the desired state of compliance. The Gap Analysis delivers a Compliance Programme Route Map with risk based prioritisation

Readiness Assessment Tool

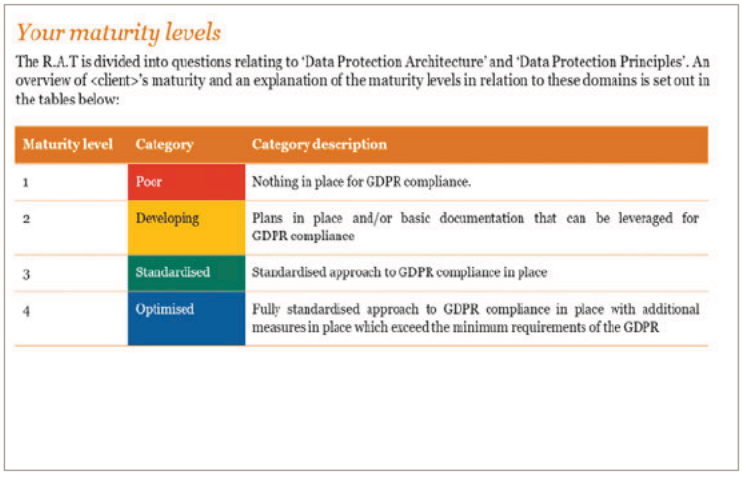
Economic sector	Geographical locations	Business plan
Culture and ethics	Risk appetite	Business operations
Programme resources and timeframe	Prior regulatory track record	Legal and organisation structure

R.A.T. results

Business operations

Enforcement tracker results

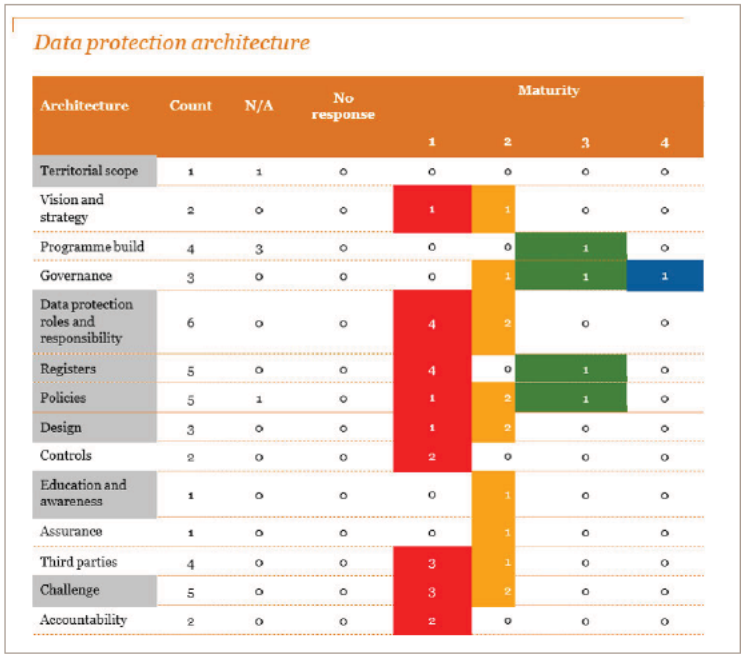
The R.A.T. report



Your maturity levels

The R.A.T is divided into questions relating to 'Data Protection Architecture' and 'Data Protection Principles'. An overview of <client>'s maturity and an explanation of the maturity levels in relation to these domains is set out in the tables below:

Maturity level	Category	Category description
1	Poor	Nothing in place for GDPR compliance.
2	Developing	Plans in place and/or basic documentation that can be leveraged for GDPR compliance
3	Standardised	Standardised approach to GDPR compliance in place
4	Optimised	Fully standardised approach to GDPR compliance in place with additional measures in place which exceed the minimum requirements of the GDPR



Data protection architecture

Architecture	Count	N/A	No response	Maturity			
				1	2	3	4
Territorial scope	1	1	0	0	0	0	0
Vision and strategy	2	0	0	1	1	0	0
Programme build	4	3	0	0	0	1	0
Governance	3	0	0	0	1	1	1
Data protection roles and responsibility	6	0	0	4	2	0	0
Registers	5	0	0	4	0	1	0
Policies	5	1	0	1	2	1	0
Design	3	0	0	1	2	0	0
Controls	2	0	0	2	0	0	0
Education and awareness	1	0	0	0	1	0	0
Assurance	1	0	0	0	1	0	0
Third parties	4	0	0	3	1	0	0
Challenge	5	0	0	3	2	0	0
Accountability	2	0	0	2	0	0	0

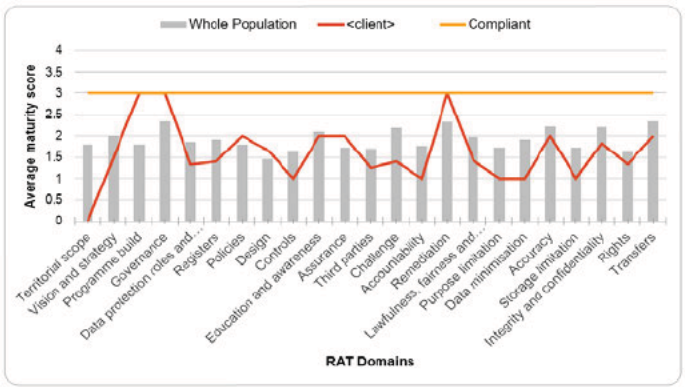
Step 3 – Change

Compliance work streams

Execution of tailored and prioritised Compliance Work Streams

Strategy and governance	**Audit and compliance**
Training and Awareness	**Data discovery and mapping**
Threat and vulnerability management	**Data remediation**
Privacy by design	**Vendor risk management**
Policy development	**Controls**
Identity and access management	**Technology and change management**

<client> vs Whole population



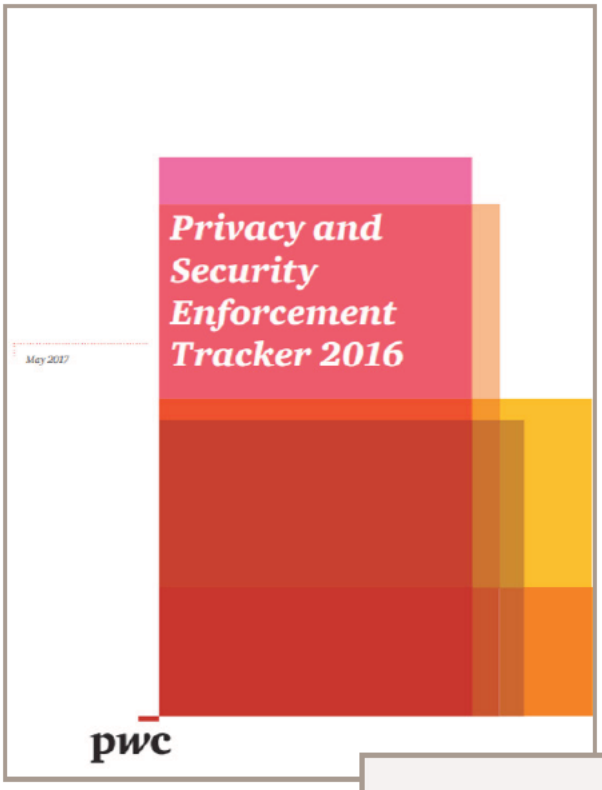
Observations

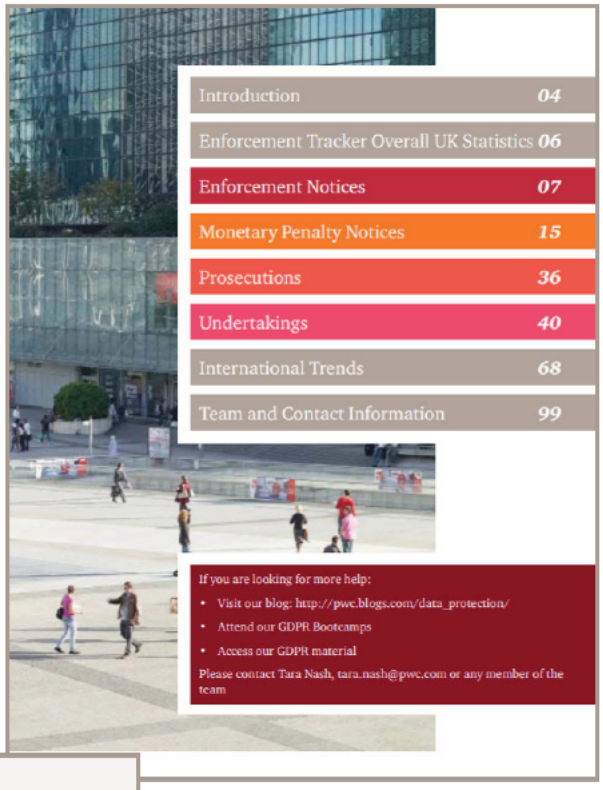
Data protection architecture

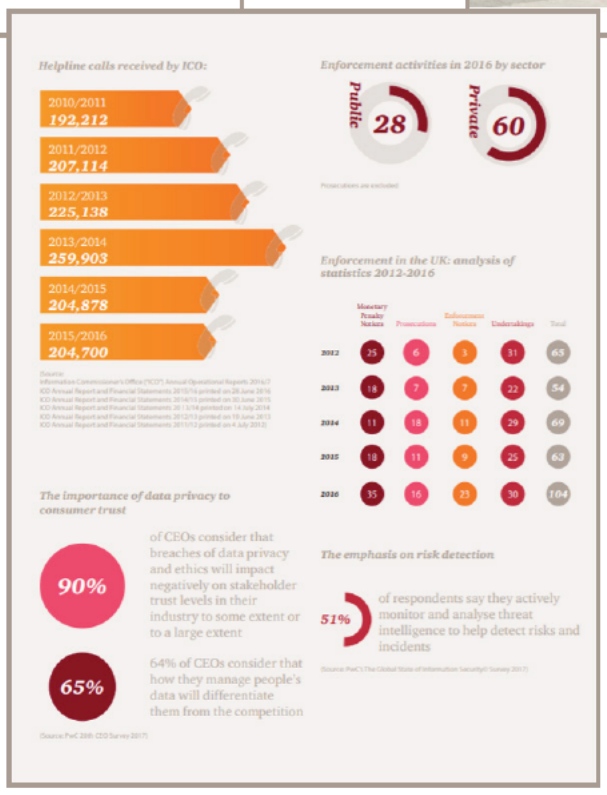
R.A.T Sub-domain	Areas that look good	Areas where there are gaps
Vision and strategy	• There is a basic vision for <client> to adhere to their requirements under the GDPR in place. This has been well communicated to the most senior members of staff across various business functions at <client>. • It was acknowledged in the workshop that the R.A.T. session and engagement with PwC was the beginning of the development of <client>'s GDPR strategy.	• <client>'s vision is not documented or detailed. It has not been communicated with the wider business. • There is currently no GDPR strategy in place at <client>.
Programme build	• <client>'s data protection programme is built on a legal basis, and uses as its foundation the Data Protection Directive 95/46/EC.	• <client>'s data protection programme is yet to be reviewed and updated in line with the new requirements under the GDPR.
Governance	• There is executive level sponsorship of <client>'s GDPR programme. Executives have a good level of involvement and knowledge of the programme's progress. • There is a GDPR steering committee which meets regularly and comprises the relevant stakeholders.	• Although some business leaders participate actively in data protection compliance activities, this is not consistent across all business leaders or the wider employee base and the involvement is ad hoc and informal.
Data protection roles and responsibility	• There is an awareness of the need to review the requirement for a DPO at <client> under the GDPR. • A new DPO is being appointed to replace the previous DPO.	• There are no other data protection roles (such as data protection champions) that have been deployed across <client>, although there are plans for these to be implemented in the near future.

The enforcement tracker

The R.A.T. includes key questions linked to Articles and Recitals of the GDPR which have been selected due to previous enforcement actions and failures of some organisations. Information from previous year's key regulatory enforcement matters can be found in our PwC Privacy and Security Enforcement Tracker which is an annual publication that includes cases in the UK and twenty other countries.







Contacts

Stewart Room
GDPR Strategy, Law and Compliance
Partner
T: +44 (0)20 7213 4306
E: stewart.room@pwc.com

Jane Wainwright
GDPR Strategy, Law and Compliance
Director
T: +44 (0)20 7212 4485
E: jane.a.wainwright@pwc.com

www.pwc.co.uk

180212-110820-MR-OS