Securys®

Global Data Privacy Experts

x

JAMAICA STOCK EXCHANGE

Digital Transformation

Treating data as an asset class

About Securys

Scale

We work globally as a specialised privacy consultancy. Our clients include some of the largest global firms in their sectors.

Locations

We have practical on-the-ground experience in most of the world's privacy regimes and know where to look for the conflicts between them.

Expertise

We bring experience of data privacy and information security assessment and remediation from multiple sectors and perspectives, as well as a formidable array of certifications across the team.

Practical approach

Our approach is strategic, risk-driven, forward looking, positive and practical – our recommendations are not theoretical or academic interpretations, they are implementable plans.

Proven methodology

Continuously evolving comprehensive audit and discovery tools with risk-scoring and flow through to dashboard and recommendations.

Securys

Founded in

2014

Offices in
UK, Europe, US and the Caribbean

Specialist expertise in FS, health, eCommerce, tourism, BPO and the industrial and energy sectors.

Clients across 70+ COUNTRIES

bsi

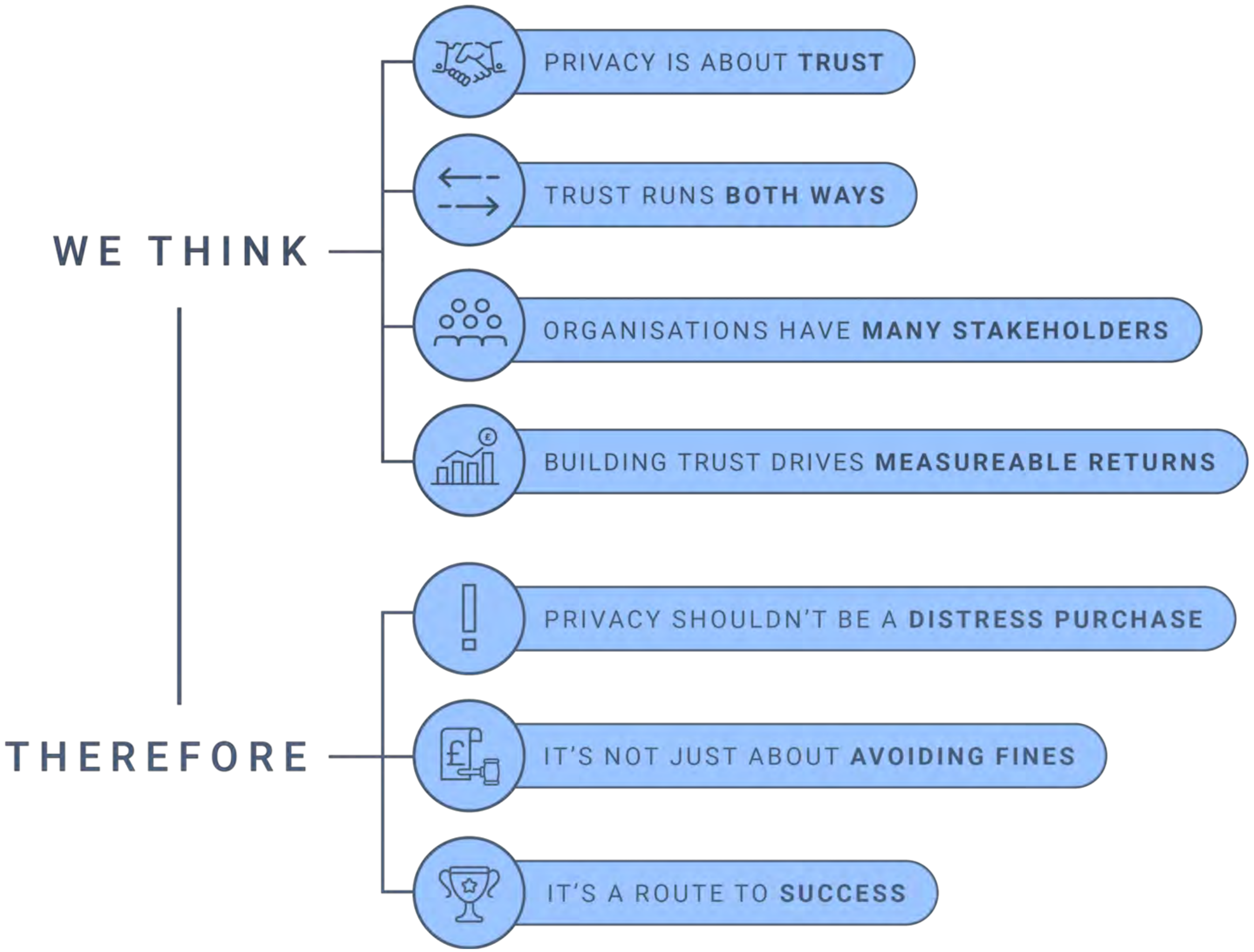
ISO/IEC
27001
Information Security
Management
CERTIFIED

ISO/IEC
27701
Privacy Information
Management
CERTIFIED

FOUNDATIONAL SUPPORTER
iappai

iapp
SILVER
MEMBER

The Value of Trust



WE THINK

PRIVACY IS ABOUT **TRUST**

TRUST RUNS **BOTH WAYS**

ORGANISATIONS HAVE **MANY STAKEHOLDERS**

BUILDING TRUST DRIVES **MEASUREABLE RETURNS**

THEREFORE

PRIVACY SHOULDN'T BE A **DISTRESS PURCHASE**

IT'S NOT JUST ABOUT **AVOIDING FINES**

IT'S A ROUTE TO **SUCCESS**

Securys®
Global Data Privacy Experts

Digital transformation

Securys®

Global Data Privacy Experts

What digital transformation isn’t

- Just digitising existing processes
- Collecting “*all* the data”, then…
- …throwing the data into a warehouse and hoping for insights
- Retrofitting dashboards and KPIs to everything
- AI…because, well, AI; I mean, everyone is doing it, right?
- Replacing customer service with chatbots

What digital transformation should be

Transforming data from a *risk* into an *asset*

Right now you have risks

- Privacy regulation
- AI regulation
- EUC sprawl
- Inaccuracy
- Disaggregation
- Excessive data sharing
- Negligent breach
- Cyber exposure

- Regulatory fines
- Reputation damage
- Litigation
- Overspend
- Customer dissatisfaction
- Inefficiency
- Poor decision-making
- Project failure

70% of transformations fail

Harry Robinson, McKinsey

What you want is measurable ROI

- Accurate and complete information
- Documented and understood processes
- Effective partner evaluation
- Measurable efficiency improvements
- Data-driven and verifiable insights
- Informed risk management
- Simplified compliance
- Competitive advantage

OK…how?

Think of data as an asset class

- ➢ You must invest in it
- ➢ You must manage it
- ➢ You must monitor its performance
- ➢ You must make lifecycle decisions

- This is not just an IT problem
- This is not just a legal problem
- This is not just a compliance problem
- …it’s a whole company opportunity
- So it’s *your* responsibility

Your role as a CEO

Put data at the heart of the enterprise

Take charge of your data governance programme

This demonstrates its importance to everyone

…shows that it’s value-adding, not a compliance cost-centre

…and keeps you fully informed of progress and opportunity

Prioritise quality over quantity

…more data is not always better

See regulation as a useful instruction manual and a toolset, not an obstacle

…at a high level the principles make obvious sense

…who wouldn’t want fairness, transparency, security and accountability?

Securys®
Global Data Privacy Experts

Our Services

Audit and discovery

- Gap analysis
- Data and process mapping
- Benchmarking

Privacy operating model

- Privacy as a service
- DPO as a service
- International transfers
- Vendor assessment
- DSAR support

Advisory and consulting

- Risk to asset transformation for data
- Data governance
- aiEthix: AI governance and regulatory compliance
- Privacy Made Positive®

www.securys.co.uk
www.securys.com.jm
www.securys.eu
www.securys.us

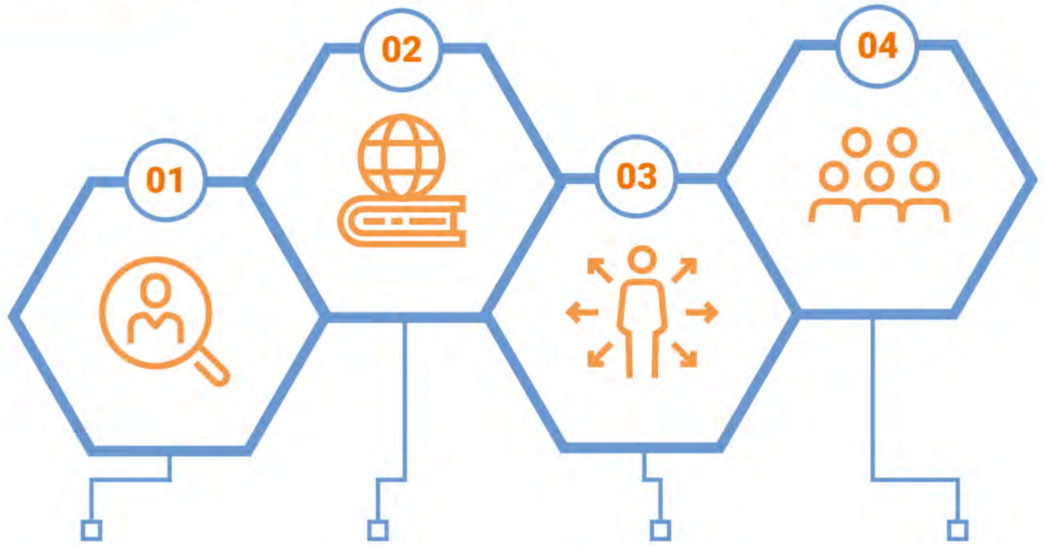
Our Services in detail

Securys®
Global Data Privacy Experts

Audit

- Validation that internal controls are working.
- Surface Risk Score™ process identifies risk and opportunities.
- RAG dashboard shows distribution of privacy risk.
- Remediation recommendations we implement with you.
- Establishes best practice.

The compliance journey



AUDIT AND DISCOVERY

- Gap analysis
- Discovery interviews
- Surface risk scoring

REPORT

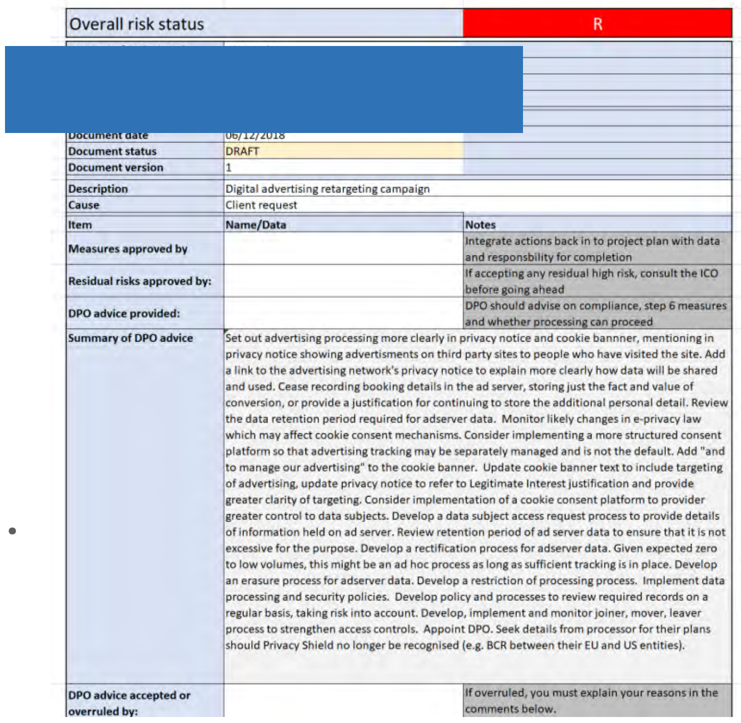
- Data catalogue and RoPA
- Risk dashboards
- Remediation recommendations

REMEDIATION

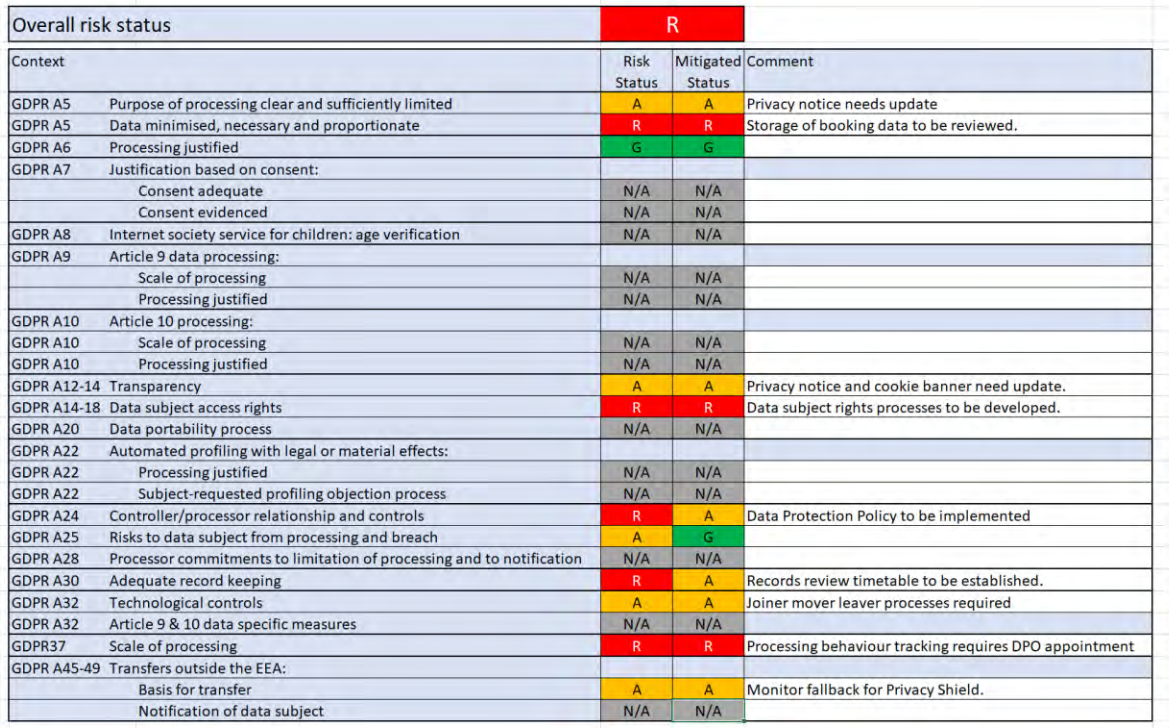
- Detailed assessments
- DPIA, LIA, TIA
- Implementation support
- Breach management

PRIVACY OFFICE

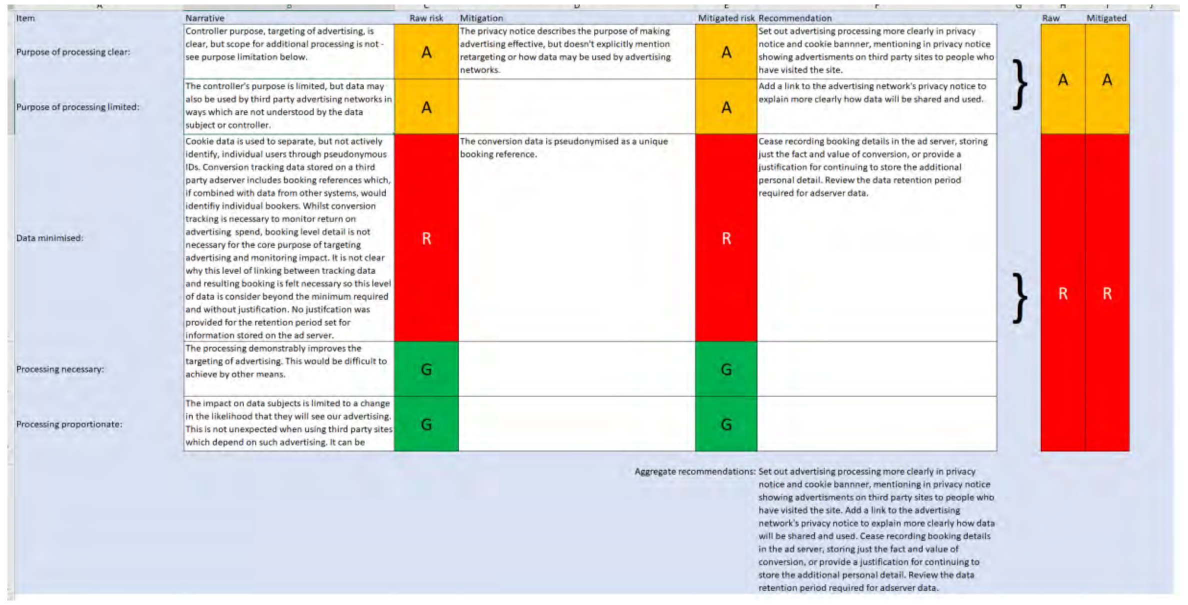
- Privacy by design
- Privacy operations
- Advice and training



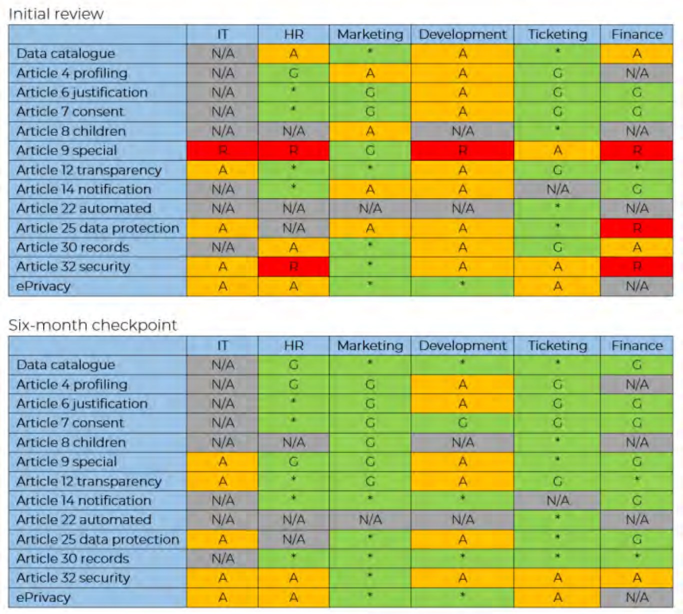
Overall risk status		R
[redacted]		
Document date	06/12/2018	
Document status	DRAFT	
Document version	1	
Description	Digital advertising retargeting campaign	
Cause	Client request	
Item	**Name/Data**	**Notes**
Measures approved by		Integrate actions back in to project plan with data and responsbility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice	Set out advertising processing more clearly in privacy notice and cookie bannner, mentioning in privacy notice showing advertisments on third party sites to people who have visited the site. Add a link to the advertising network's privacy notice to explain more clearly how data will be shared and used. Cease recording booking details in the ad server, storing just the fact and value of conversion, or provide a justification for continuing to store the additional personal detail. Review the data retention period required for adserver data. Monitor likely changes in e-privacy law which may affect cookie consent mechanisms. Consider implementing a more structured consent platform so that advertising tracking may be separately managed and is not the default. Add "and to manage our advertising" to the cookie banner. Update cookie banner text to include targeting of advertising, update privacy notice to refer to Legitimate Interest justification and provide greater clarity of targeting. Consider implementation of a cookie consent platform to provider greater control to data subjects. Develop a data subject access request process to provide details of information held on ad server. Review retention period of ad server data to ensure that it is not excessive for the purpose. Develop a rectification process for adserver data. Given expected zero to low volumes, this might be an ad hoc process as long as sufficient tracking is in place. Develop an erasure process for adserver data. Develop a restriction of processing process. Implement data processing and security policies. Develop policy and processes to review required records on a regular basis, taking risk into account. Develop, implement and monitor joiner, mover, leaver process to strengthen access controls. Appoint DPO. Seek details from processor for their plans should Privacy Shield no longer be recognised (e.g. BCR between their EU and US entities).	
DPO advice accepted or overruled by:		If overruled, you must explain your reasons in the comments below.



Overall risk status		R		
Context		Risk Status	Mitigated Status	Comment
GDPR A5	Purpose of processing clear and sufficiently limited	A	A	Privacy notice needs update
GDPR A5	Data minimised, necessary and proportionate	R	R	Storage of booking data to be reviewed.
GDPR A6	Processing justified	G	G	
GDPR A7	Justification based on consent:			
	Consent adequate	N/A	N/A	
	Consent evidenced	N/A	N/A	
GDPR A8	Internet society service for children: age verification	N/A	N/A	
GDPR A9	Article 9 data processing:			
	Scale of processing	N/A	N/A	
	Processing justified	N/A	N/A	
GDPR A10	Article 10 processing:			
GDPR A10	Scale of processing	N/A	N/A	
GDPR A10	Processing justified	N/A	N/A	
GDPR A12-14	Transparency	A	A	Privacy notice and cookie banner need update.
GDPR A14-18	Data subject access rights	R	R	Data subject rights processes to be developed.
GDPR A20	Data portability process	N/A	N/A	
GDPR A22	Automated profiling with legal or material effects:			
GDPR A22	Processing justified	N/A	N/A	
GDPR A22	Subject-requested profiling objection process	N/A	N/A	
GDPR A24	Controller/processor relationship and controls	R	A	Data Protection Policy to be implemented
GDPR A25	Risks to data subject from processing and breach	A	G	
GDPR A28	Processor commitments to limitation of processing and to notification	N/A	N/A	
GDPR A30	Adequate record keeping	R	A	Records review timetable to be established.
GDPR A32	Technological controls	A	A	Joiner mover leaver processes required
GDPR A32	Article 9 & 10 data specific measures	N/A	N/A	
GDPR37	Scale of processing	R	R	Processing behaviour tracking requires DPO appointment
GDPR A45-49	Transfers outside the EEA:			
	Basis for transfer	A	A	Monitor fallback for Privacy Shield.
	Notification of data subject	N/A	N/A	



A	B	C	D	E	F	G	H	I
Item	Narrative	Raw risk	Mitigation	Mitigated risk	Recommendation		Raw	Mitigated
Purpose of processing clear:	Controller purpose, targeting of advertising, is clear, but scope for additional processing is not - see purpose limitation below.	A	The privacy notice describes the purpose of making advertising effective, but doesn't explicitly mention retargeting or how data may be used by advertising networks.	A	Set out advertising processing more clearly in privacy notice and cookie bannner, mentioning in privacy notice showing advertisments on third party sites to people who have visited the site.	}	A	A
Purpose of processing limited:	The controller's purpose is limited, but data may also be used by third party advertising networks in ways which are not understood by the data subject or controller.	A		A	Add a link to the advertising network's privacy notice to explain more clearly how data will be shared and used.			
Data minimised:	Cookie data is used to separate, but not actively identify, individual users through pseudonymous IDs. Conversion tracking data stored on a third party adserver includes booking references which, if combined with data from other systems, would identifiy individual bookers. Whilst conversion tracking is necessary to monitor return on advertising spend, booking level detail is not necessary for the core purpose of targeting advertising and monitoring impact. It is not clear why this level of linking between tracking data and resulting booking is felt necessary so this level of data is consider beyond the minimum required and without justification. No justifcation was provided for the retention period set for information stored on the ad server.	R	The conversion data is pseudonymised as a unique booking reference.	R	Cease recording booking details in the ad server, storing just the fact and value of conversion, or provide a justification for continuing to store the additional personal detail. Review the data retention period required for adserver data.	}	R	R
Processing necessary:	The processing demonstrably improves the targeting of advertising. This would be difficult to achieve by other means.	G		G				
Processing proportionate:	The impact on data subjects is limited to a change in the likelihood that they will see our advertising. This is not unexpected when using third party sites which depend on such advertising. It can be	G		G				
				Aggregate recommendations:	Set out advertising processing more clearly in privacy notice and cookie bannner, mentioning in privacy notice showing advertisments on third party sites to people who have visited the site. Add a link to the advertising network's privacy notice to explain more clearly how data will be shared and used. Cease recording booking details in the ad server, storing just the fact and value of conversion, or provide a justification for continuing to store the additional personal detail. Review the data retention period required for adserver data.			



Initial review

	IT	HR	Marketing	Development	Ticketing	Finance
Data catalogue	N/A	A	*	A	*	A
Article 4 profiling	N/A	G	A	A	G	N/A
Article 6 justification	N/A	*	G	A	G	G
Article 7 consent	N/A	*	G	A	G	G
Article 8 children	N/A	N/A	A	N/A	*	N/A
Article 9 special	R	R	G	R	A	R
Article 12 transparency	A	*	*	A	G	*
Article 14 notification	N/A	*	A	A	N/A	G
Article 22 automated	N/A	N/A	N/A	N/A	*	N/A
Article 25 data protection	A	N/A	A	A	*	R
Article 30 records	N/A	A	*	A	G	A
Article 32 security	A	R	*	A	A	R
ePrivacy	A	A	*	*	A	N/A

Six-month checkpoint

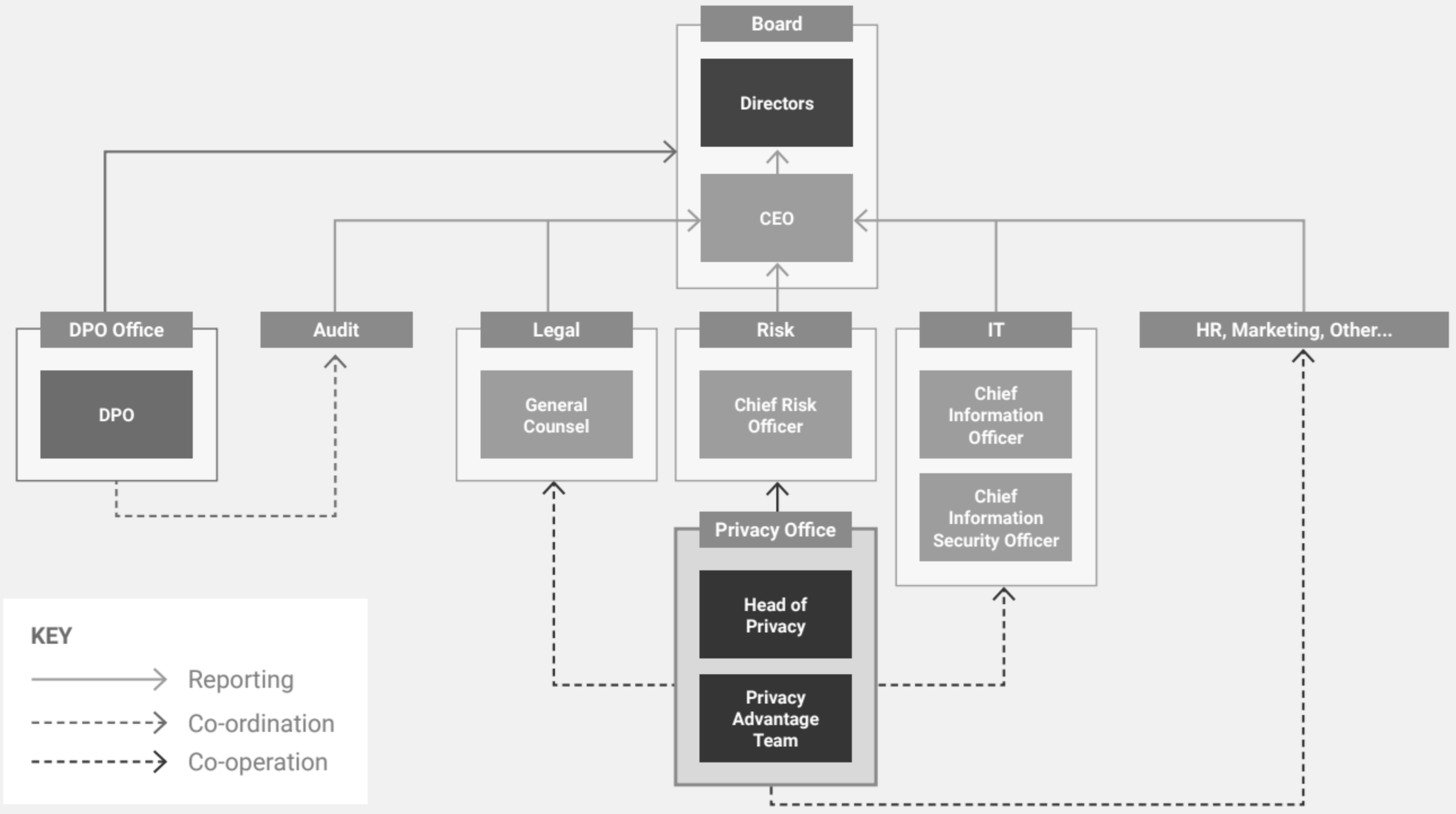
	IT	HR	Marketing	Development	Ticketing	Finance
Data catalogue	N/A	G	*	*	*	G
Article 4 profiling	N/A	G	G	A	G	N/A
Article 6 justification	N/A	*	G	A	G	G
Article 7 consent	N/A	*	G	G	G	G
Article 8 children	N/A	N/A	G	N/A	*	N/A
Article 9 special	A	G	G	A	*	G
Article 12 transparency	A	*	G	A	G	*
Article 14 notification	N/A	*	*	*	N/A	G
Article 22 automated	N/A	N/A	N/A	N/A	*	N/A
Article 25 data protection	A	N/A	*	A	*	G
Article 30 records	N/A	*	*	*	*	*
Article 32 security	A	A	*	A	A	A
ePrivacy	A	A	*	*	A	N/A

Privacy Operating Model

- Addressing the key challenge facing organisations - how to define and institute a privacy operating model which supports the organisations.
- Cohesion with key functions.
- Ensures privacy function is fully integrated into wider governance.
- Flexible and adaptable.
- Fosters the privacy advantage.

A successful privacy operating model underwrites practical privacy with good governance and places trust and transparency at the heart of data protection.

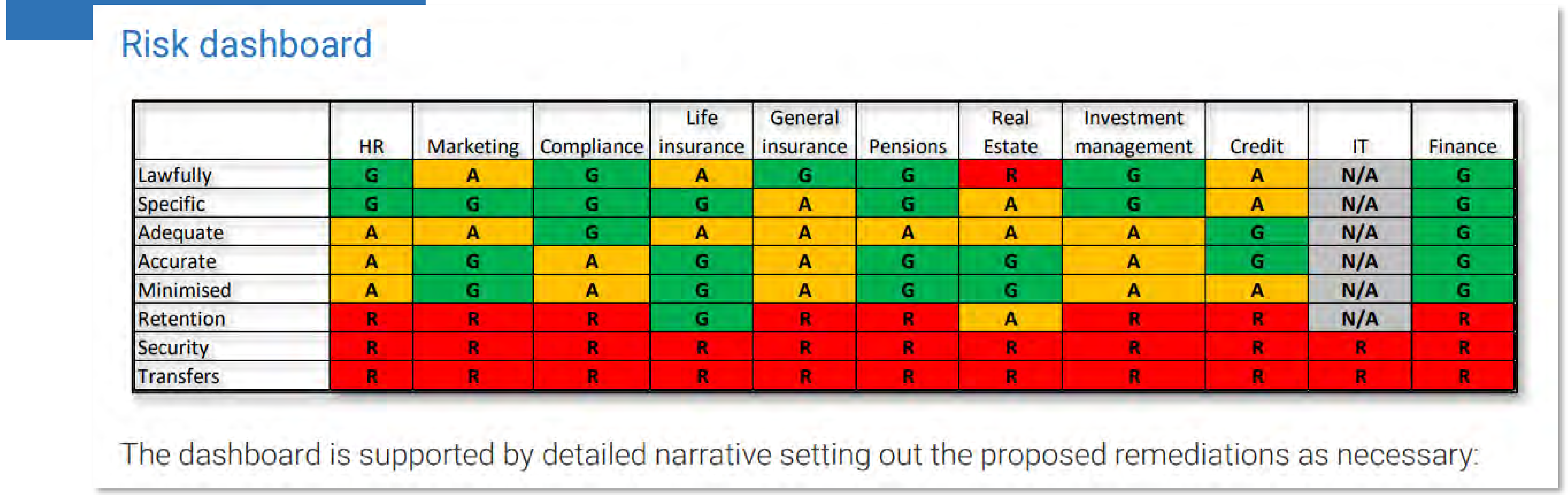
DPO and Privacy Office: Sample organisational structure



Privacy as a service – Outsourced Support

- Outsource while retaining governance.
- Framework for data protection compliance:
  - Discovery and risk evaluation
  - Remediation
  - Ongoing data protection support.
- Fully resourced.
- Ready access to expert advice.
- Privacy by design and default.

You get continuously updated, drillable view of privacy risk across the enterprise and regular reporting to drop into your governance style.



Risk dashboard

	HR	Marketing	Compliance	Life insurance	General insurance	Pensions	Real Estate	Investment management	Credit	IT	Finance
Lawfully	G	A	G	A	G	G	R	G	A	N/A	G
Specific	G	G	G	G	A	G	A	G	A	N/A	G
Adequate	A	A	G	A	A	A	A	A	G	N/A	G
Accurate	A	G	A	G	A	G	G	A	G	N/A	G
Minimised	A	G	A	G	A	G	G	A	A	N/A	G
Retention	R	R	R	G	R	R	A	R	R	N/A	R
Security	R	R	R	R	R	R	R	R	R	R	R
Transfers	R	R	R	R	R	R	R	R	R	R	R

The dashboard is supported by detailed narrative setting out the proposed remediations as necessary:

DPO as a service

- Our DPO as a service included advice, guidance, training and breach support.
- Flexible and adaptable service to protect personal data and oversee your regulatory compliance.
- Designated DPO assigned to your team.
- DPO is a Certified Privacy Professional and is up-to-date with privacy and information security landscape.
- Support for broad range of needs including handling data subject enquiries.
- Pre-existing best practice templates for required policy and procedure documentation.
- Strong track record of working with similar clients in your sector.

Policies and procedures

Our assisted compliance service, providing maintenance of all the necessary records, including Data Protection Impact Assessments, records of data processing and privacy-related policies.

Breach response

Investigation, breach recording, crisis communications and breach mitigation. On-site or remote response with a cast-iron SLA to ensure that you meet your regulatory reporting requirements.

Governance

Independent monitoring and oversight of your data processing in line with regulatory requirements, accurate record keeping and regular assessment of the impact of your policies through on-site audit visits and assurance reports.

Communication

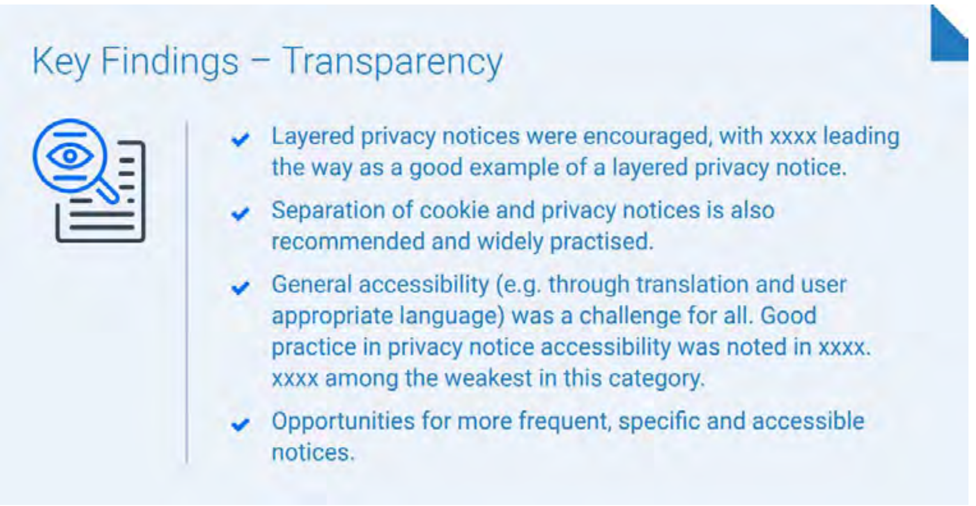
Liaison with the ICO and other relevant regulators, direct handling of data subject access requests and other enquires; dealing with suppliers and customers including review of data sharing agreements.

Helping manage your data protection whilst meeting all regulatory requirements.

Benchmarking

- Privacy benchmarking exercise shows how your approach to privacy compares when rated against peers in your sector and the wider world.
- Exercise considers your privacy maturity as well as competitors, partners and other organisations.
- Detailed report with improvement recommendations.

Our benchmarking service is the foundation for organisations looking to improve their competitive position on privacy.

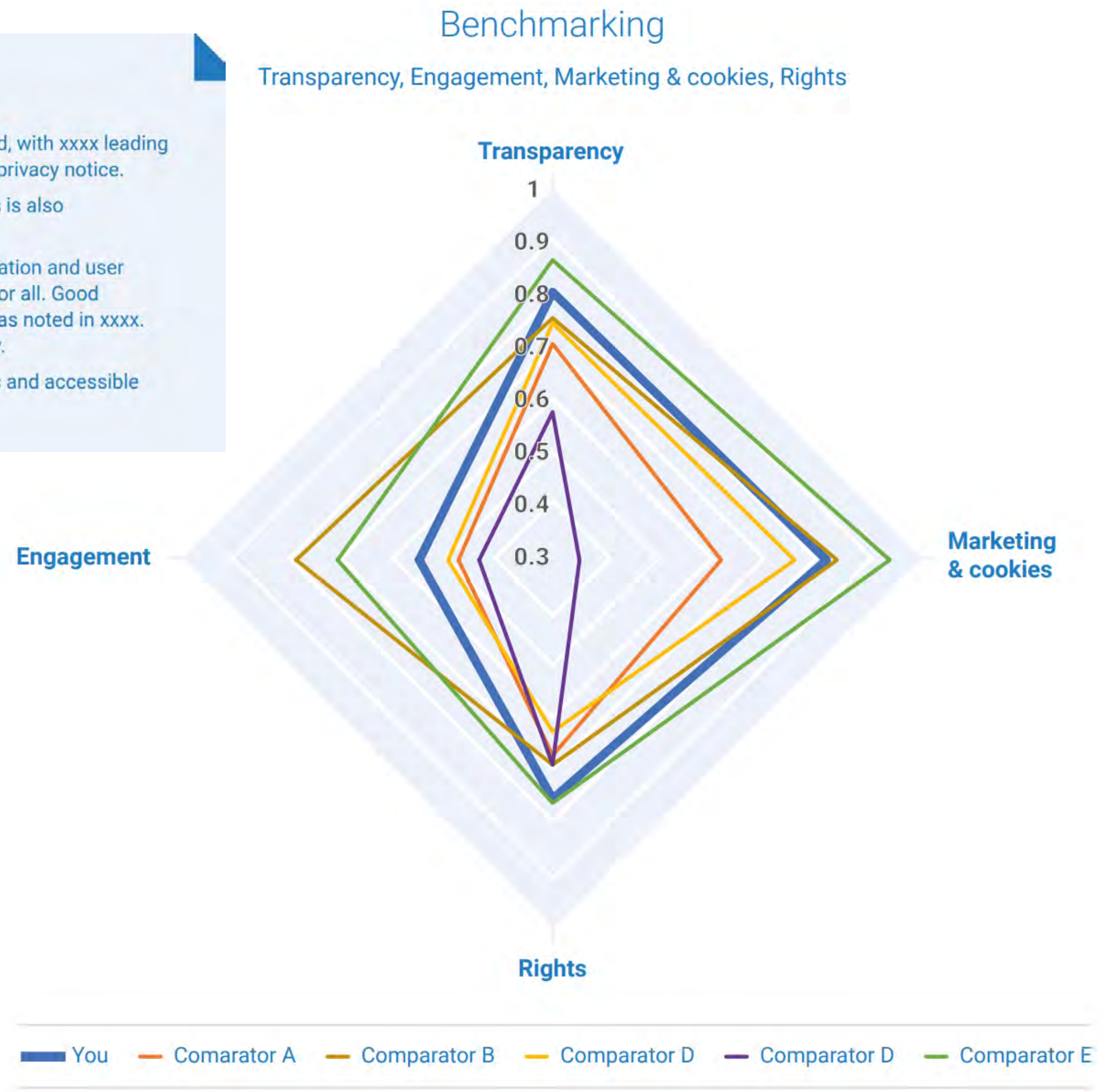


Key Findings – Transparency

- ✓ Layered privacy notices were encouraged, with xxxx leading the way as a good example of a layered privacy notice.
- ✓ Separation of cookie and privacy notices is also recommended and widely practised.
- ✓ General accessibility (e.g. through translation and user appropriate language) was a challenge for all. Good practice in privacy notice accessibility was noted in xxxx. xxxx among the weakest in this category.
- ✓ Opportunities for more frequent, specific and accessible notices.

Sample findings

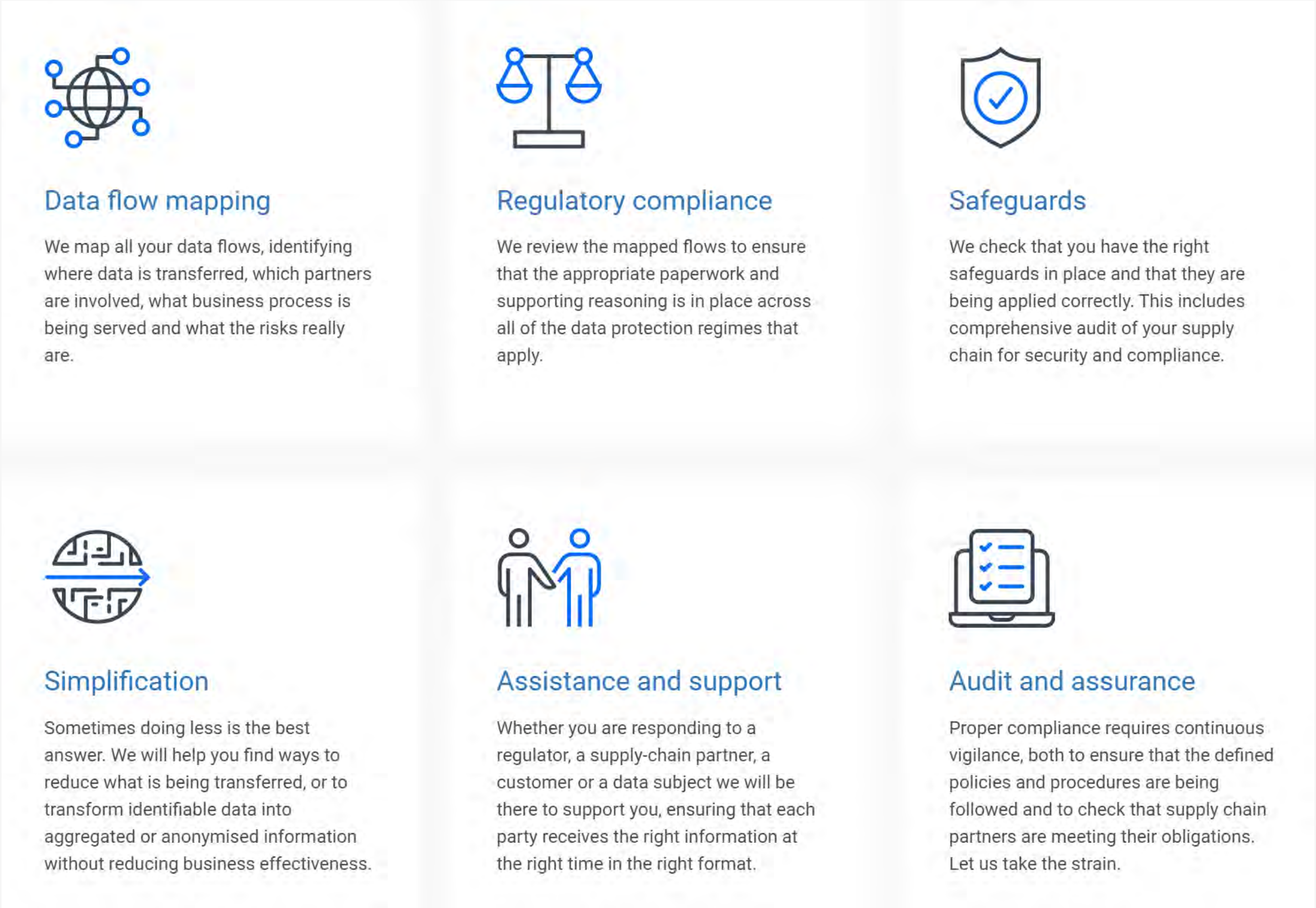
Figure 2: Sample radar chart that provides multi-axis comparison to demonstrate privacy maturity versus competitors.



International Data Transfers

- For business to operate effectively, data needs to flow internationally.
- Laws and regulations are complex and constantly changing.
- We help you understand, quantify and treat transfer risk.
- Service includes audit, remediation, maintenance.
- We add value by leveraging data protection to improve business processes and simplify your compliance regime.
- We mitigate compliance risk and ensure the productivity of your business operations.

> *A comprehensive service that ensures data subject rights are protected whilst keeping data flowing and risks minimised.*



Data flow mapping

We map all your data flows, identifying where data is transferred, which partners are involved, what business process is being served and what the risks really are.

Regulatory compliance

We review the mapped flows to ensure that the appropriate paperwork and supporting reasoning is in place across all of the data protection regimes that apply.

Safeguards

We check that you have the right safeguards in place and that they are being applied correctly. This includes comprehensive audit of your supply chain for security and compliance.

Simplification

Sometimes doing less is the best answer. We will help you find ways to reduce what is being transferred, or to transform identifiable data into aggregated or anonymised information without reducing business effectiveness.

Assistance and support

Whether you are responding to a regulator, a supply-chain partner, a customer or a data subject we will be there to support you, ensuring that each party receives the right information at the right time in the right format.

Audit and assurance

Proper compliance requires continuous vigilance, both to ensure that the defined policies and procedures are being followed and to check that supply chain partners are meeting their obligations. Let us take the strain.

DSAR Support

- Flexible service, tailored to specific organisational need.
- Scalable according to demand.
- Calibrated to clients’ available internal resources.
- All forms of rights request for all types of client.
- Service available immediately/at short notice.
- Appropriate resource for the task.
- Reporting and review to promote cycle of constant improvement.

Supporting strained resources

Streamlined process

Best practice

Building trust

Global expertise

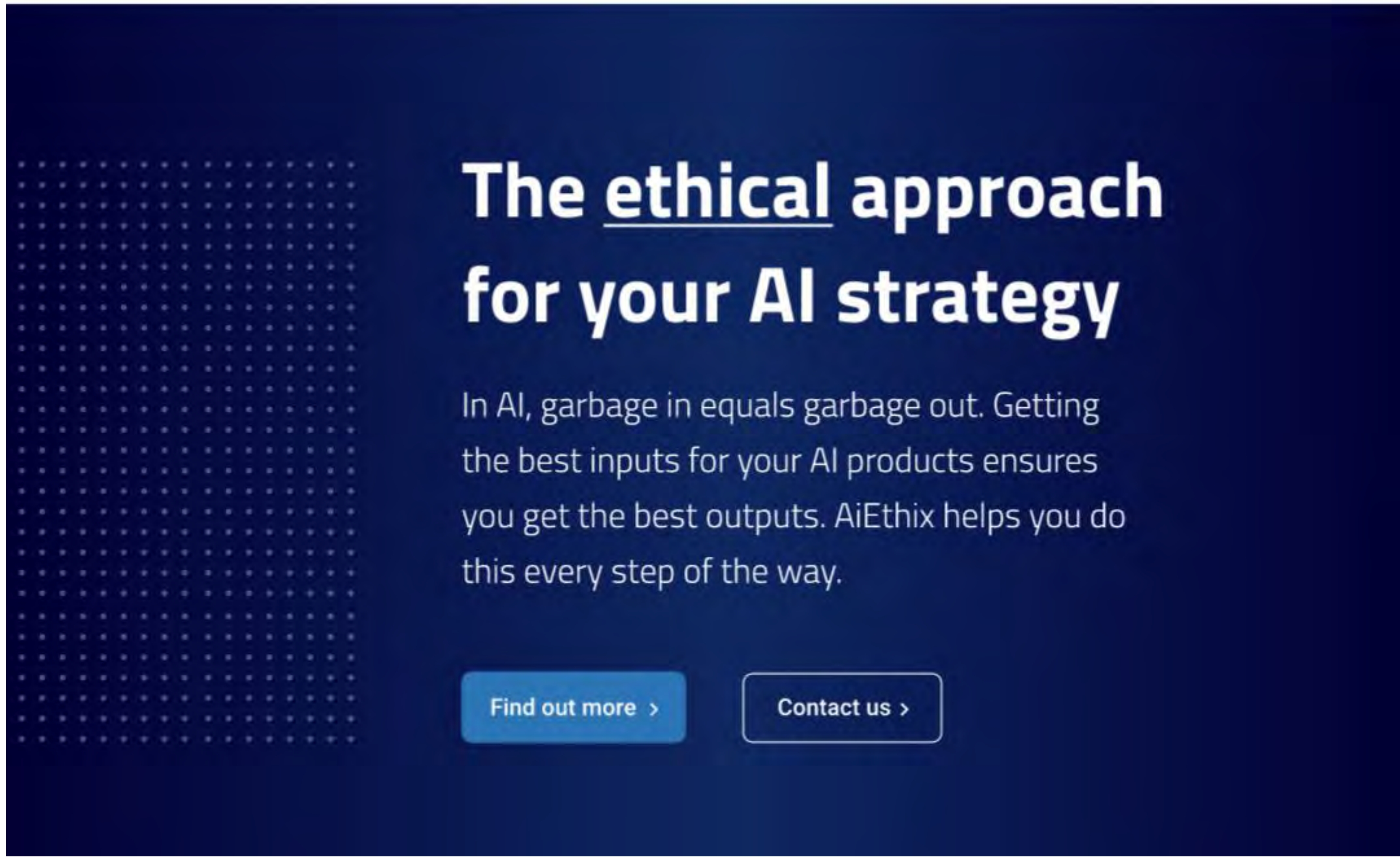
Consulting

- Flexible service, tailored to specific organisational need.
- Our consultants combine extensive privacy knowledge with real-world commercial experience.
- Strategy, advice and design right to delivery and maintenance.
- Privacy, cyber, regulatory and commercial compliance.
- Scalable according to demand.
- Calibrated to clients’ available internal resources.
- Service available immediately/at short notice.
- Effective resource to manage complexity.

AI/ML Services

- Specialist AI and data privacy consulting
    - Expert insight into data governance, risk management and data privacy
- Three core offerings
    - AI discovery
    - AI-by-design
    - AI governance
- What do we bring
    - Global knowledge, locally delivered
    - Deep data protection expertise
    - Practical approach
- Ensure alignment with enacted AI legislation
- Keep you fully informed of forthcoming legislation

aiEthix
from Securys



The ethical approach for your AI strategy

In AI, garbage in equals garbage out. Getting the best inputs for your AI products ensures you get the best outputs. AiEthix helps you do this every step of the way.

How We Work

Our Mission and Values

Securys is a specialist consultancy focused on the human side of data protection and information security.

We use our wide and deep experience of cyber, data protection, regulation and governance to bring a strongly practical and positive approach to helping businesses, charities and other organisations of all sizes to protect themselves and their stakeholders.

Collectively our team has every relevant data privacy and information security certification, including CIPP/E, CIPP/A, CIPM, CIPT, CIPP/US, CISSP, ISSMP, CISA, FIP, FBCS & CITP.

More importantly we have decades of collective experience in management and governance.

- We're committed to doing good, not merely doing well.
- We believe that technology should be a positive contributor to society.
- We believe that not just privacy but control of one's personal data is a fundamental right.
- We believe that ethics come before profits, and that good stewardship of data is a duty.
- We help our clients earn and retain the trust of all their stakeholders.

Our approach

- People-first approach that builds trust whilst being creative and collaborative.
- The belief that privacy has a positive value is a key foundation of our practice.
- We make privacy work for you.
- We work with you to look for the best ways of managing risk and achieving your business goals.
- Integrated and comprehensive service.
- Privacy-by-design at the core of our approach.

Making privacy work to your advantage.

DRIVE SUCCESS

Delivering privacy in a global context means going beyond privacy box-ticking. Beyond customers. Beyond fines. We combine legal, cyber and corporate capabilities to help enterprises address all of their stakeholders and enable the foundations for growth.

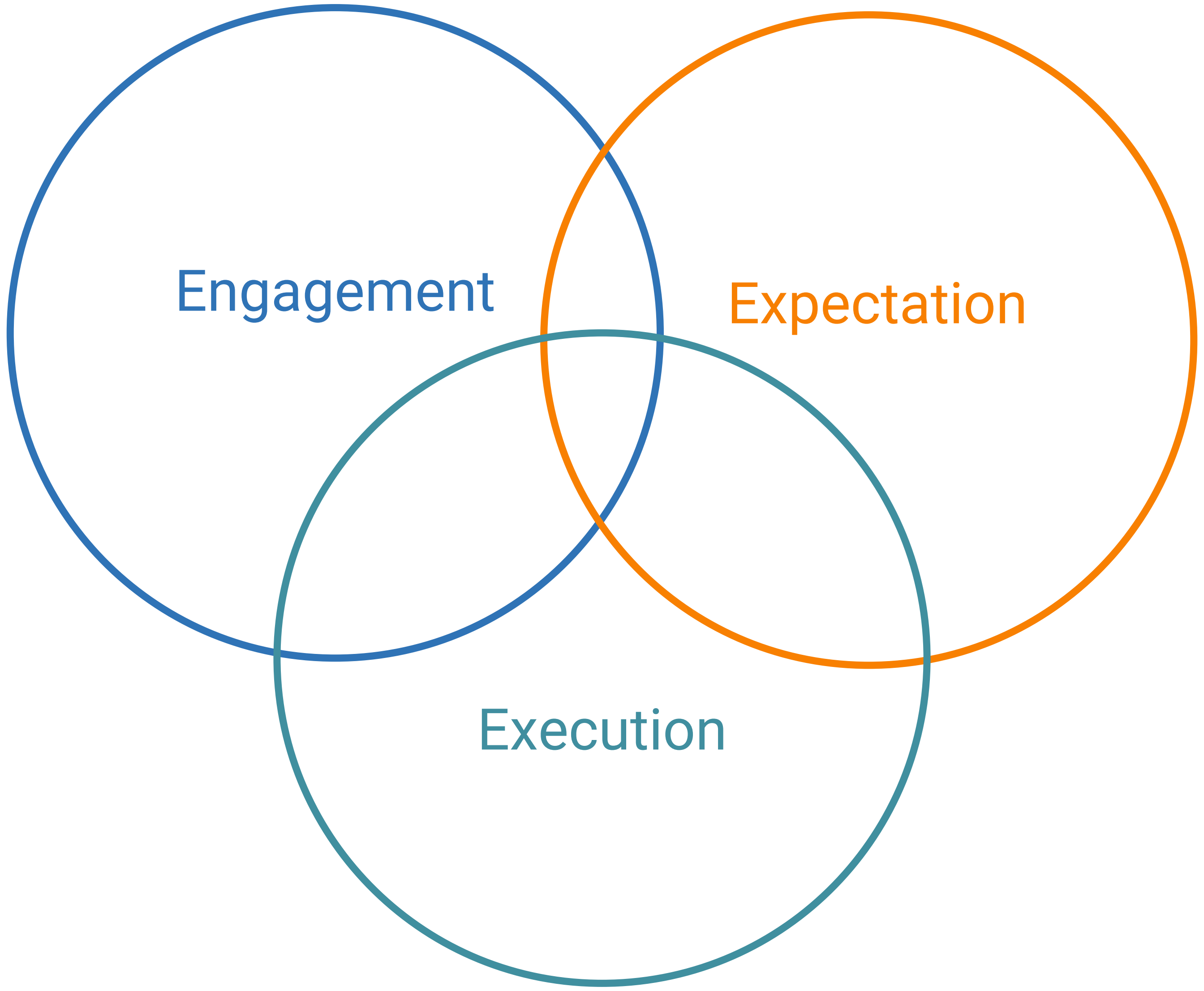
REDUCE RISK

We uncover risks that our clients may not even have been aware of. As industry specialists, we understand the depth and parameters of risks that our competitors may not. And by helping our clients mitigate these, we can also enable them to build business confidence.

BUILD TRUST

We help our clients to build trust that brings a wide variety of benefits – Including better talent acquisition, improvements in employee loyalty and retention rates, increases in net promoter scores, stronger commercial partnerships and measurable sales success.

What drives success?



Engagement

Board and executive commitment
Need for compliance and ethics sold in throughout the organisation
Privacy and security embedded in everyone’s role objectives

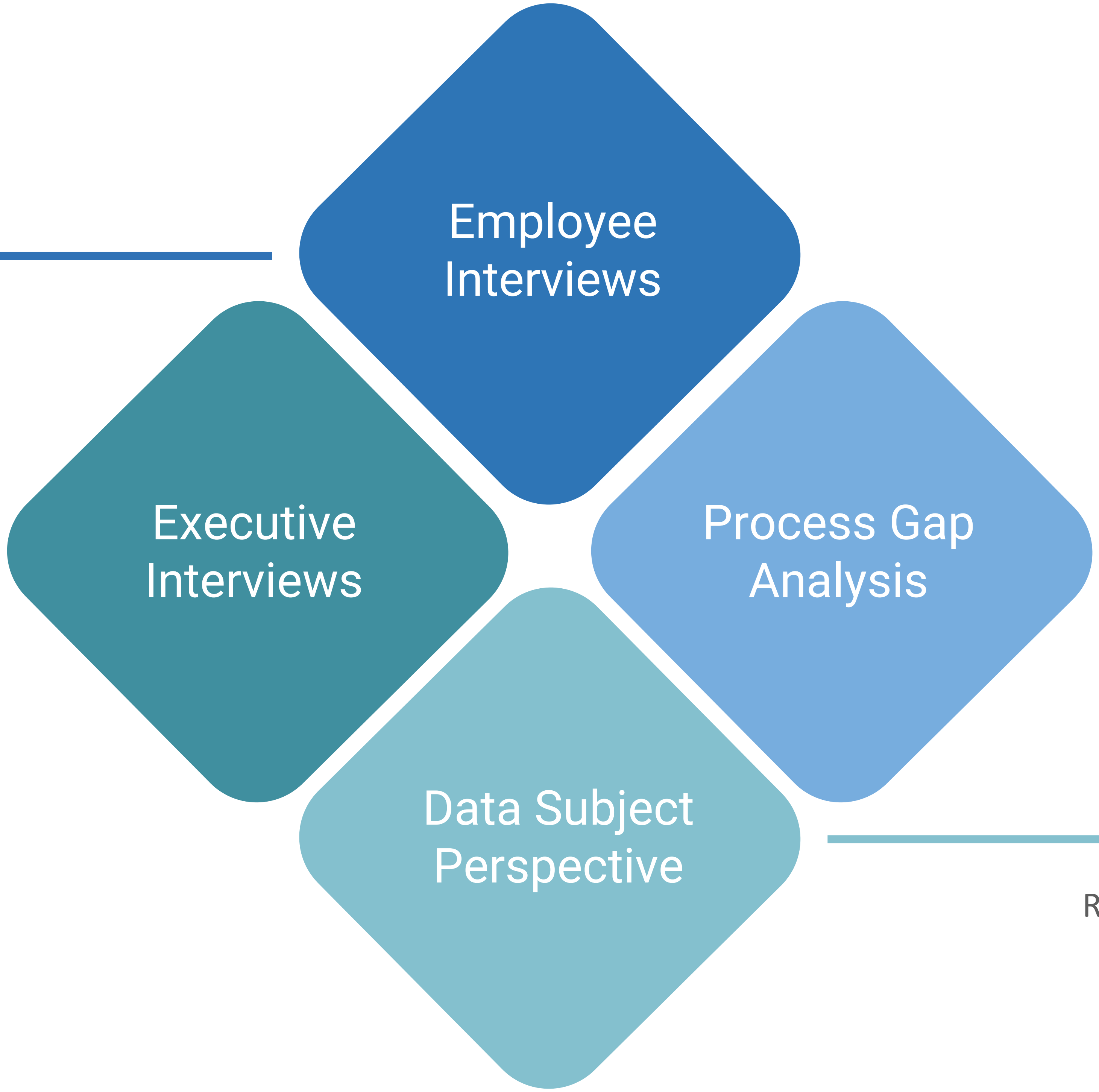
Expectation

have a realistic view of the status quo
be seekers after truth, not merely look for box ticks or reinforcement; accept and budget for the need for change

Execution

information should be a two-way flow
mesh practical suggestions with identification of non-compliance
avoid silos and work in a privacy-security-supply chain continuum

How we engage



Employee Interviews

Speak to employees who deal with data to assess their understanding of privacy and regulation.

Executive Interviews

Meet with executives with privacy accountability – understand their concerns and KPIs.

Process Gap Analysis

Review client’s record of processing activities – compare to best practice and identify gaps.

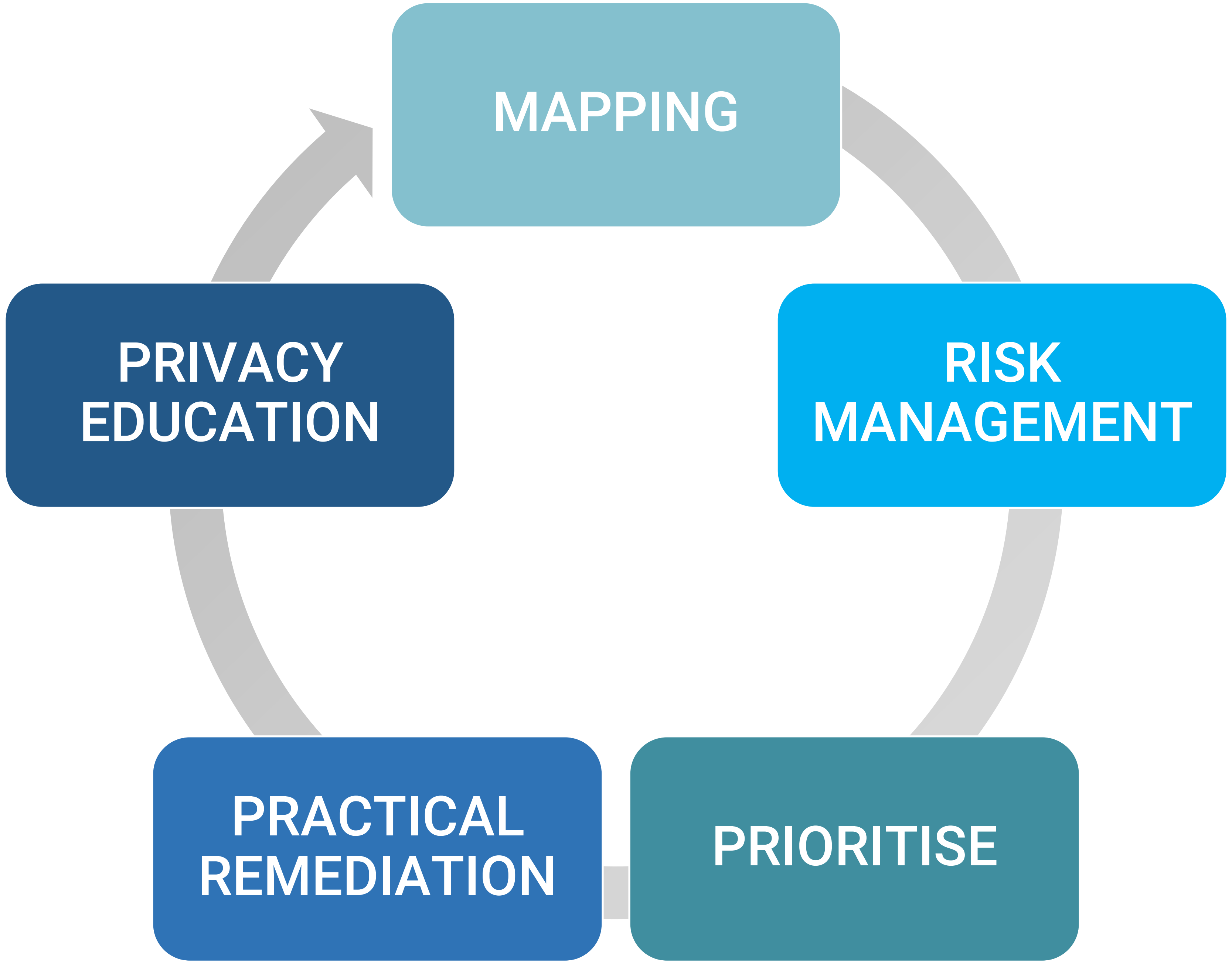
Data Subject Perspective

Review public- and employee-facing privacy notices for completeness and compliance.

Securys®
Global Data Privacy Experts

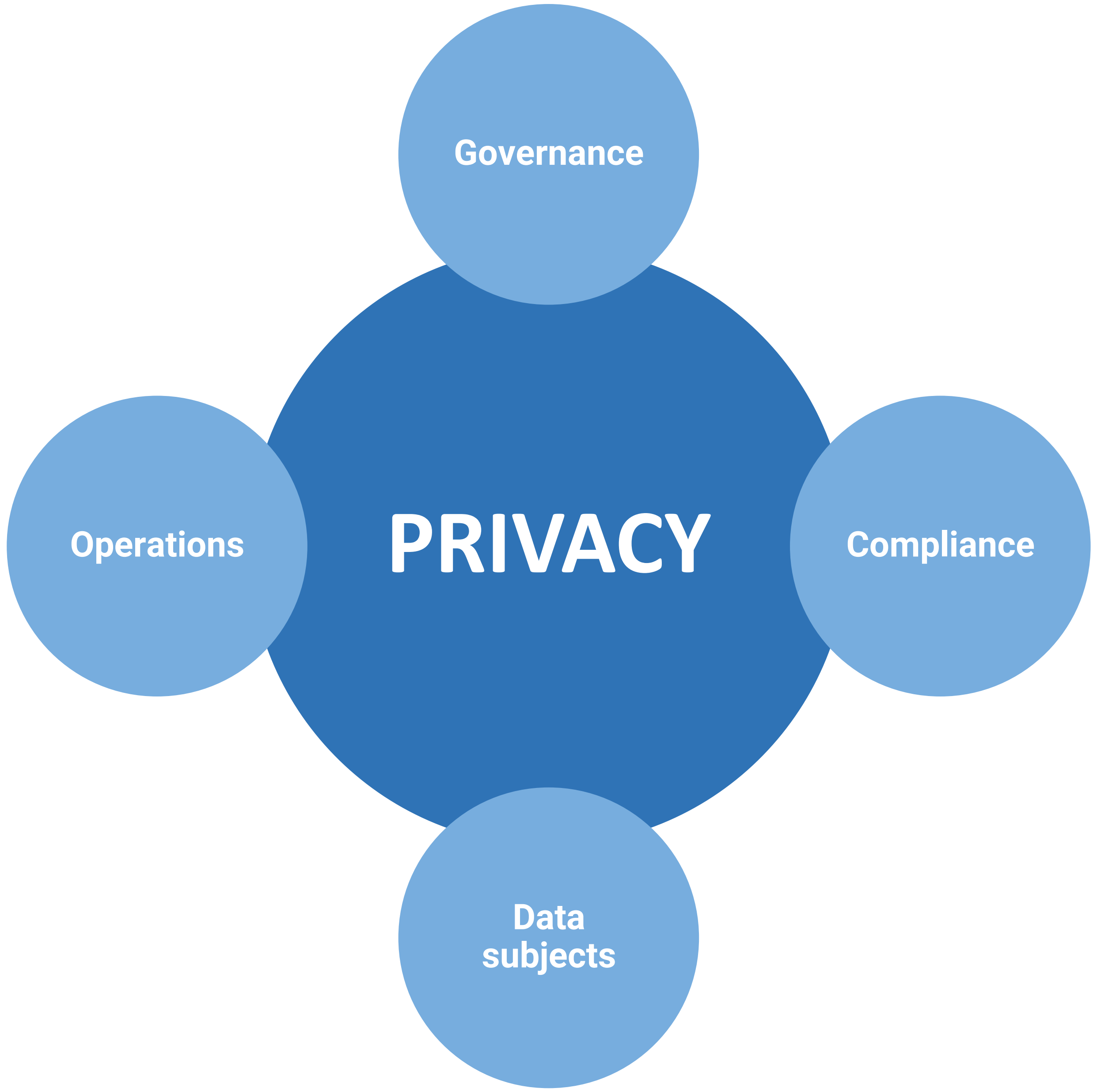
How we set expectations

- Privacy is a process and a culture, not a destination.
- The privacy office is a collaborative function, neither a box-ticker nor a blocker.
- Identify and address your processes in risk-prioritised order.

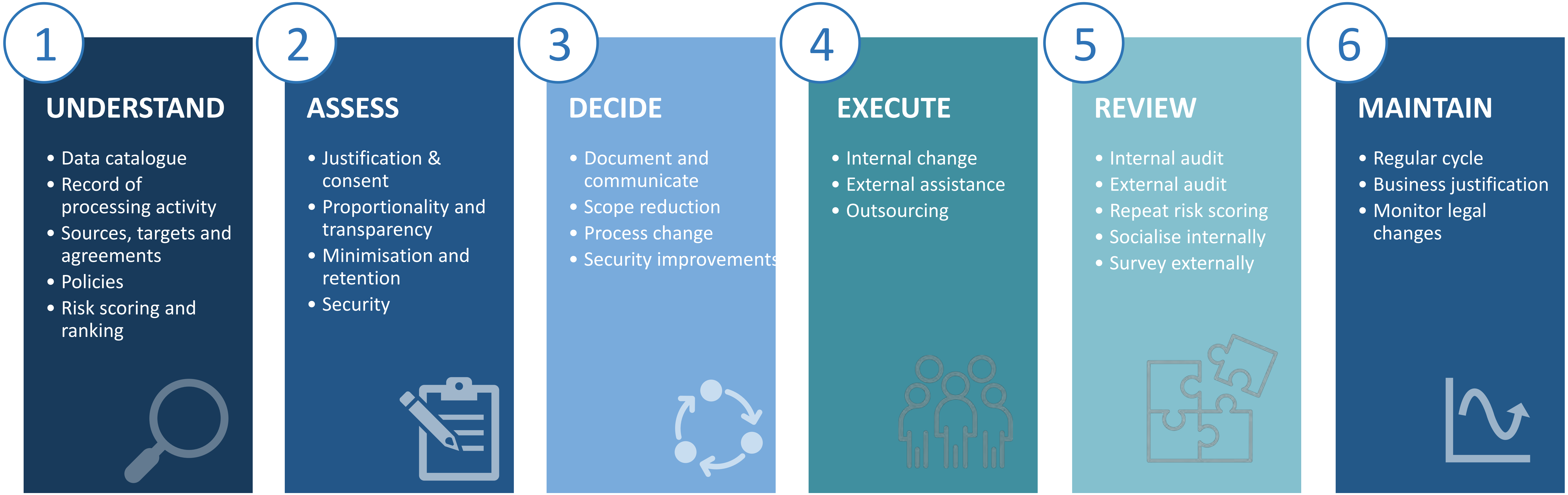


How we set expectations

- Work top-down to develop appropriate governance.
- Work with operational teams to embed privacy culture.
- Work with compliance to build the continuum view of regulation.
- Work with data subjects to build trust through transparency.



How we execute



1 UNDERSTAND

- Data catalogue
- Record of processing activity
- Sources, targets and agreements
- Policies
- Risk scoring and ranking

2 ASSESS

- Justification & consent
- Proportionality and transparency
- Minimisation and retention
- Security

3 DECIDE

- Document and communicate
- Scope reduction
- Process change
- Security improvements

4 EXECUTE

- Internal change
- External assistance
- Outsourcing

5 REVIEW

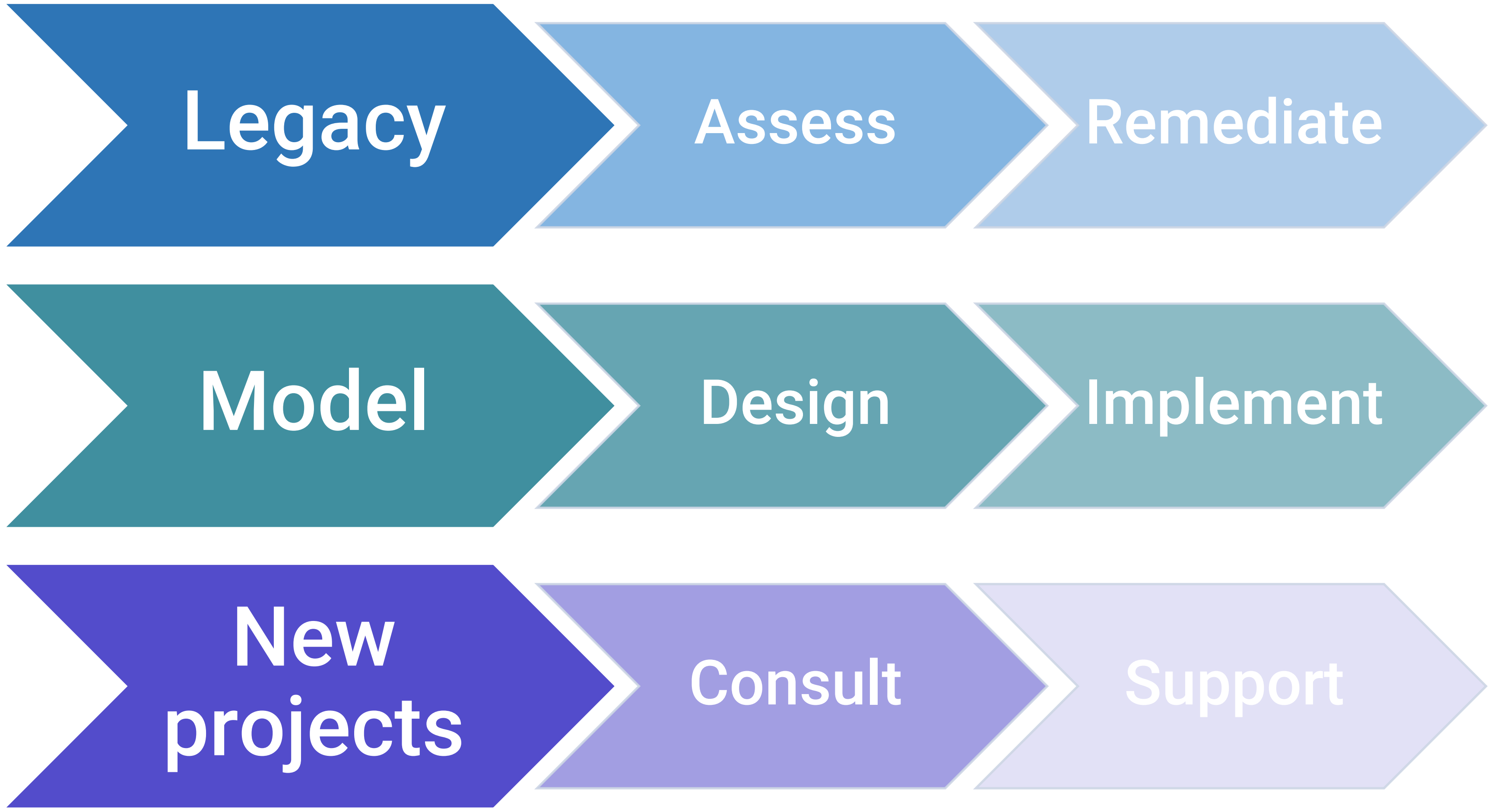
- Internal audit
- External audit
- Repeat risk scoring
- Socialise internally
- Survey externally

6 MAINTAIN

- Regular cycle
- Business justification
- Monitor legal changes

How we execute

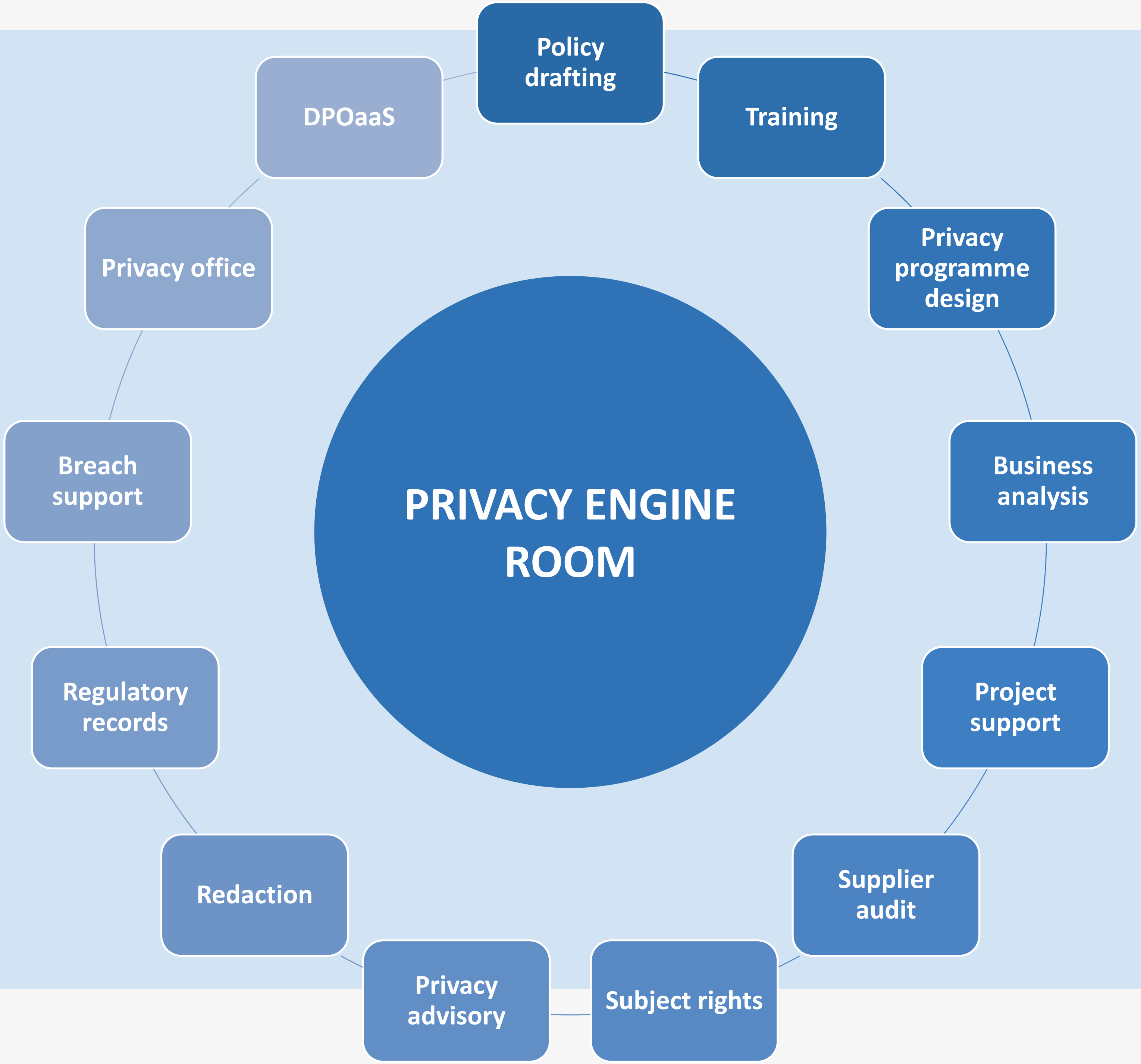
- Multiple workstreams
- Focused teams, each led by a practice lead
- Combine design, training, support and operational delivery as required
- Close integration with the client



A flexible operating model

Support for in-house privacy professionals

Project assistance and resource

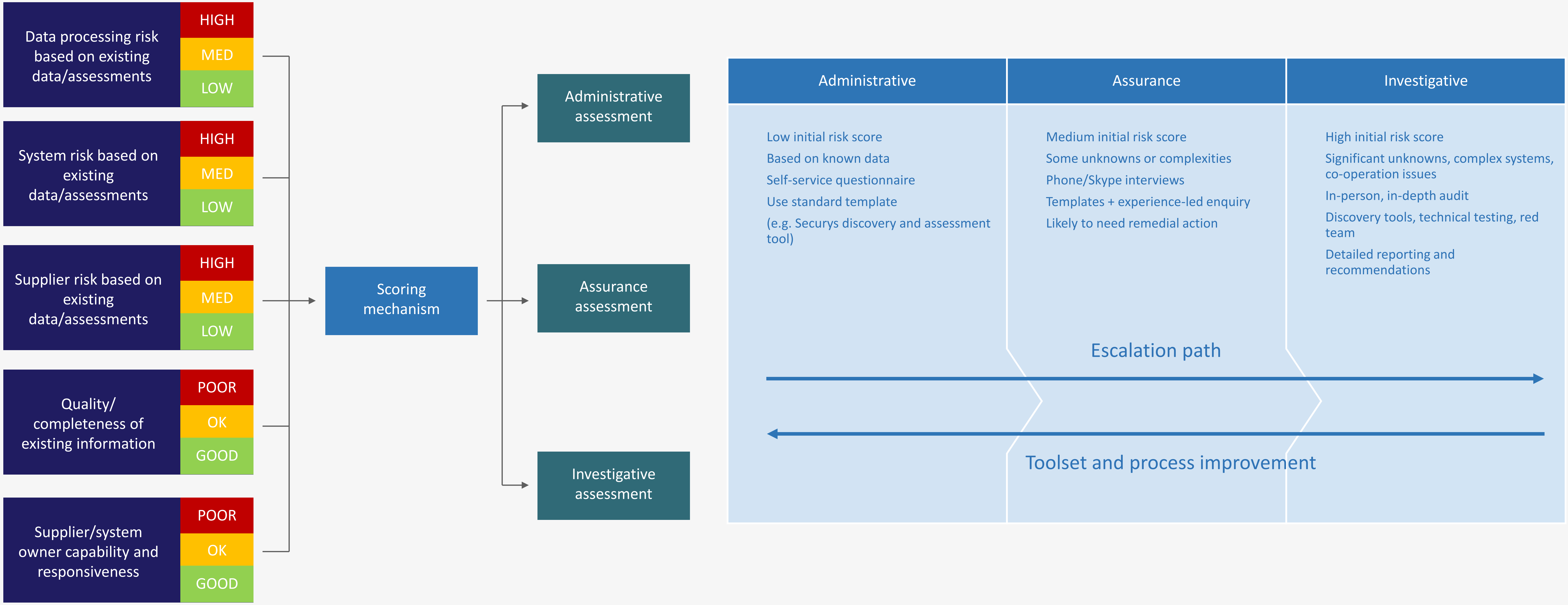


Audit and validation

Full privacy outsource

Securys®
Global Data Privacy Experts

A risk-based approach



Data processing risk based on existing data/assessments	HIGH MED LOW
System risk based on existing data/assessments	HIGH MED LOW
Supplier risk based on existing data/assessments	HIGH MED LOW
Quality/ completeness of existing information	POOR OK GOOD
Supplier/system owner capability and responsiveness	POOR OK GOOD

Scoring mechanism

Administrative assessment

Assurance assessment

Investigative assessment

Administrative	Assurance	Investigative
Low initial risk score Based on known data Self-service questionnaire Use standard template (e.g. Securys discovery and assessment tool)	Medium initial risk score Some unknowns or complexities Phone/Skype interviews Templates + experience-led enquiry Likely to need remedial action	High initial risk score Significant unknowns, complex systems, co-operation issues In-person, in-depth audit Discovery tools, technical testing, red team Detailed reporting and recommendations

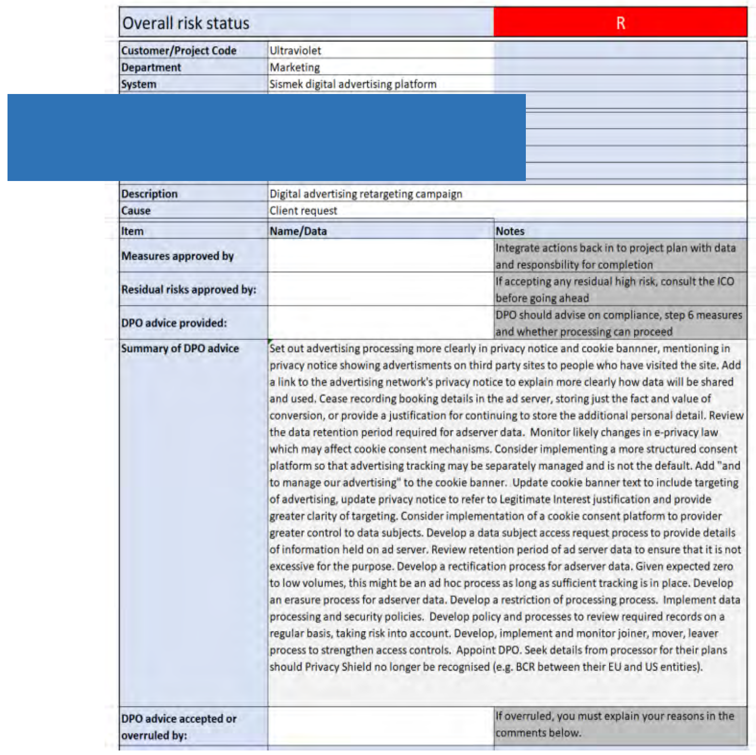
Escalation path

Toolset and process improvement

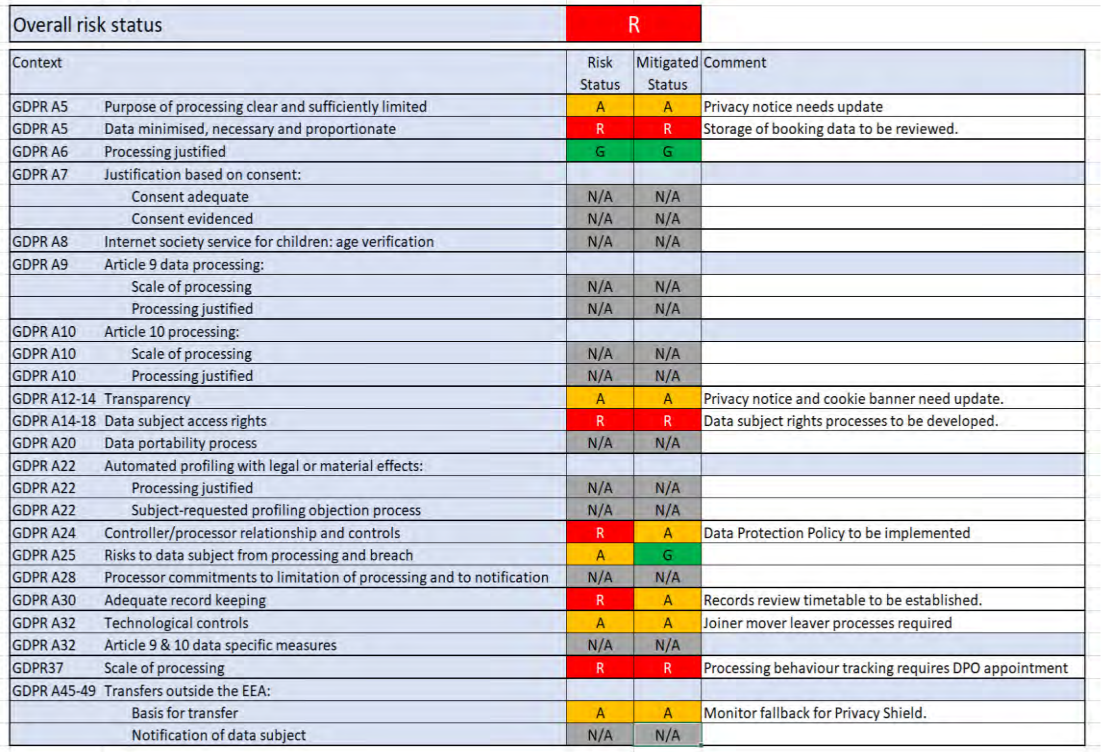
Securys
Global Data Privacy Experts

Proprietary tools

Continuously evolving comprehensive audit and discovery tools with risk-scoring and flow-through to dashboard and recommendations.

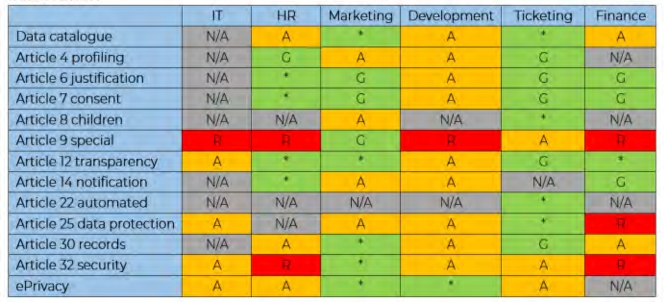


Overall risk status		R
Customer/Project Code	Ultraviolet	
Department	Marketing	
System	Sismek digital advertising platform	
[redacted]		
Description	Digital advertising retargeting campaign	
Cause	Client request	
Item	**Name/Data**	**Notes**
Measures approved by		Integrate actions back in to project plan with data and responsbility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice	Set out advertising processing more clearly in privacy notice and cookie bannner, mentioning in privacy notice showing advertisments on third party sites to people who have visited the site. Add a link to the advertising network's privacy notice to explain more clearly how data will be shared and used. Cease recording booking details in the ad server, storing just the fact and value of conversion, or provide a justification for continuing to store the additional personal detail. Review the data retention period required for adserver data. Monitor likely changes in e-privacy law which may affect cookie consent mechanisms. Consider implementing a more structured consent platform so that advertising tracking may be separately managed and is not the default. Add "and to manage our advertising" to the cookie banner. Update cookie banner text to include targeting of advertising, update privacy notice to refer to Legitimate Interest justification and provide greater clarity of targeting. Consider implementation of a cookie consent platform to provider greater control to data subjects. Develop a data subject access request process to provide details of information held on ad server. Review retention period of ad server data to ensure that it is not excessive for the purpose. Develop a rectification process for adserver data. Given expected zero to low volumes, this might be an ad hoc process as long as sufficient tracking is in place. Develop an erasure process for adserver data. Develop a restriction of processing process. Implement data processing and security policies. Develop policy and processes to review required records on a regular basis, taking risk into account. Develop, implement and monitor joiner, mover, leaver process to strengthen access controls. Appoint DPO. Seek details from processor for their plans should Privacy Shield no longer be recognised (e.g. BCR between their EU and US entities).	
DPO advice accepted or overruled by:		If overruled, you must explain your reasons in the comments below.



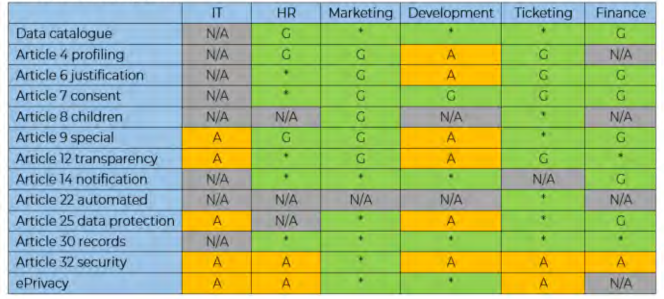
Overall risk status		R		
Context		Risk Status	Mitigated Status	Comment
GDPR A5	Purpose of processing clear and sufficiently limited	A	A	Privacy notice needs update
GDPR A5	Data minimised, necessary and proportionate	R	R	Storage of booking data to be reviewed.
GDPR A6	Processing justified	G	G	
GDPR A7	Justification based on consent:			
	Consent adequate	N/A	N/A	
	Consent evidenced	N/A	N/A	
GDPR A8	Internet society service for children: age verification	N/A	N/A	
GDPR A9	Article 9 data processing:			
	Scale of processing	N/A	N/A	
	Processing justified	N/A	N/A	
GDPR A10	Article 10 processing:			
GDPR A10	Scale of processing	N/A	N/A	
GDPR A10	Processing justified	N/A	N/A	
GDPR A12-14	Transparency	A	A	Privacy notice and cookie banner need update.
GDPR A14-18	Data subject access rights	R	R	Data subject rights processes to be developed.
GDPR A20	Data portability process	N/A	N/A	
GDPR A22	Automated profiling with legal or material effects:			
GDPR A22	Processing justified	N/A	N/A	
GDPR A22	Subject-requested profiling objection process	N/A	N/A	
GDPR A24	Controller/processor relationship and controls	R	A	Data Protection Policy to be implemented
GDPR A25	Risks to data subject from processing and breach	A	G	
GDPR A28	Processor commitments to limitation of processing and to notification	N/A	N/A	
GDPR A30	Adequate record keeping	R	A	Records review timetable to be established.
GDPR A32	Technological controls	A	A	Joiner mover leaver processes required
GDPR A32	Article 9 & 10 data specific measures	N/A	N/A	
GDPR37	Scale of processing	R	R	Processing behaviour tracking requires DPO appointment
GDPR A45-49	Transfers outside the EEA:			
	Basis for transfer	A	A	Monitor fallback for Privacy Shield.
	Notification of data subject	N/A	N/A	

Initial review

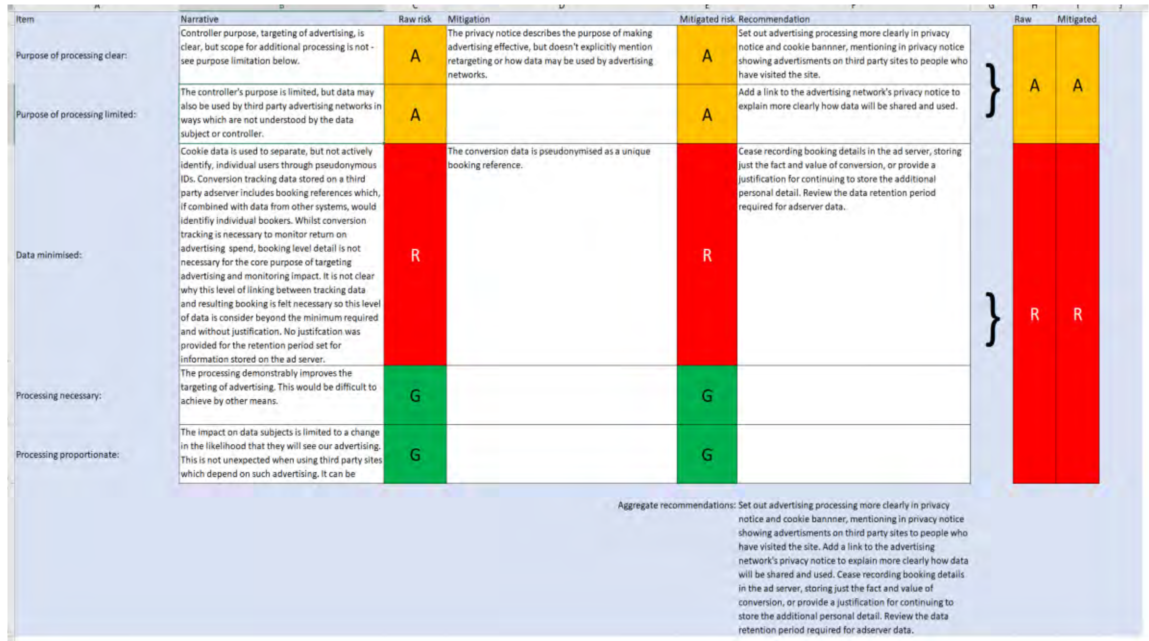


	IT	HR	Marketing	Development	Ticketing	Finance
Data catalogue	N/A	A	*	A	*	A
Article 4 profiling	N/A	G	A	A	G	N/A
Article 6 justification	N/A	*	G	A	G	G
Article 7 consent	N/A	*	G	A	G	G
Article 8 children	N/A	N/A	A	N/A	*	N/A
Article 9 special	R	R	G	R	A	R
Article 12 transparency	A	*	*	A	G	*
Article 14 notification	N/A	*	A	A	N/A	G
Article 22 automated	N/A	N/A	N/A	N/A	*	N/A
Article 25 data protection	A	N/A	A	A	*	R
Article 30 records	N/A	A	*	A	G	A
Article 32 security	A	R	*	A	A	R
ePrivacy	A	A	*	*	A	N/A

Six-month checkpoint



	IT	HR	Marketing	Development	Ticketing	Finance
Data catalogue	N/A	G	*	*	*	G
Article 4 profiling	N/A	G	G	A	G	N/A
Article 6 justification	N/A	*	G	A	G	G
Article 7 consent	N/A	*	G	G	G	G
Article 8 children	N/A	N/A	G	N/A	*	N/A
Article 9 special	A	G	G	A	*	G
Article 12 transparency	A	*	G	A	G	*
Article 14 notification	N/A	*	*	*	N/A	G
Article 22 automated	N/A	N/A	N/A	N/A	*	N/A
Article 25 data protection	A	N/A	*	A	*	G
Article 30 records	N/A	*	*	*	*	*
Article 32 security	A	A	*	A	A	A
ePrivacy	A	A	*	*	A	N/A



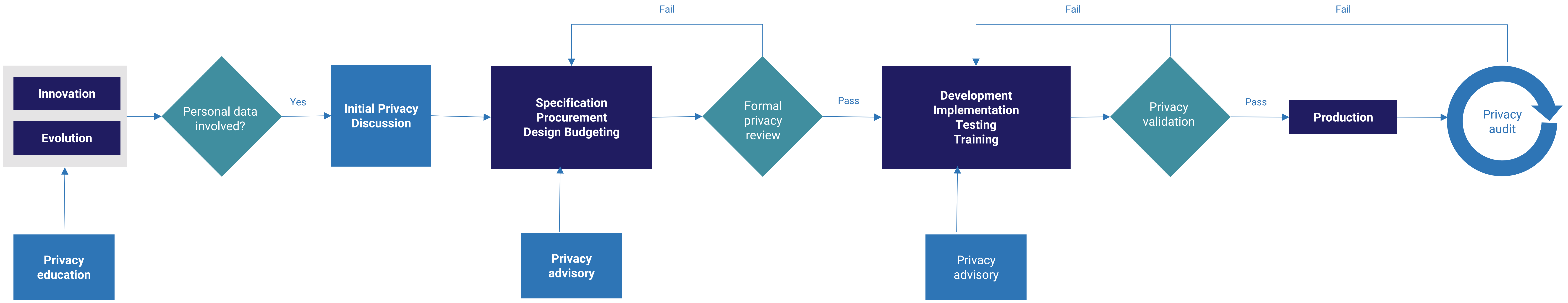
Item	Narrative	Raw risk	Mitigation	Mitigated risk	Recommendation		Raw	Mitigated
Purpose of processing clear:	Controller purpose, targeting of advertising, is clear, but scope for additional processing is not - see purpose limitation below.	A	The privacy notice describes the purpose of making advertising effective, but doesn't explicitly mention retargeting or how data may be used by advertising networks.	A	Set out advertising processing more clearly in privacy notice and cookie bannner, mentioning in privacy notice showing advertisments on third party sites to people who have visited the site.	}	A	A
Purpose of processing limited:	The controller's purpose is limited, but data may also be used by third party advertising networks in ways which are not understood by the data subject or controller.	A		A	Add a link to the advertising network's privacy notice to explain more clearly how data will be shared and used.			
Data minimised:	Cookie data is used to separate, but not actively identify, individual users through pseudonymous IDs. Conversion tracking data stored on a third party adserver includes booking references which, if combined with data from other systems, would identifiy individual bookers. Whilst conversion tracking is necessary to monitor return on advertising spend, booking level detail is not necessary for the core purpose of targeting advertising and monitoring impact. It is not clear why this level of linking between tracking data and resulting booking is felt necessary so this level of data is consider beyond the minimum required and without justification. No justifcation was provided for the retention period set for information stored on the ad server.	R	The conversion data is pseudonymised as a unique booking reference.	R	Cease recording booking details in the ad server, storing just the fact and value of conversion, or provide a justification for continuing to store the additional personal detail. Review the data retention period required for adserver data.	}	R	R
Processing necessary:	The processing demonstrably improves the targeting of advertising. This would be difficult to achieve by other means.	G		G				
Processing proportionate:	The impact on data subjects is limited to a change in the likelihood that they will see our advertising. This is not unexpected when using third party sites which depend on such advertising. It can be	G		G				

Aggregate recommendations: Set out advertising processing more clearly in privacy notice and cookie bannner, mentioning in privacy notice showing advertisments on third party sites to people who have visited the site. Add a link to the advertising network's privacy notice to explain more clearly how data will be shared and used. Cease recording booking details in the ad server, storing just the fact and value of conversion, or provide a justification for continuing to store the additional personal detail. Review the data retention period required for adserver data.

Securys®

Global Data Privacy Experts

Privacy by design



Securys®
Global Data Privacy Experts

Privacy Made Positive ®

Securys®
Global Data Privacy Experts

Privacy Made Positive®

- Using privacy as a competitive advantage to drive success.
- An ongoing research project:
  - Economic and statistical analysis
  - Consumer and employee research
  - Investor analysis.
- Dedicated research hub at www.privacymadepostive.com

Privacy Made Positive® research

Privacy Made Positive® is a manifesto, a research programme and a set of tools to help organisations profit from improving privacy.

Privacy Made Positive® allows an organisation to go beyond compliance and use privacy and trust as a marketing tool.

Phase 1
Economic Research

Desk research conducted to provide evidence of the positive value that following good privacy practices adds to a business.

Phase 2
Europe Research

Research with 4,000 consumers across the UK, France, Germany and Ireland to assess their attitudes towards privacy and to ascertain how privacy has impacted their buying behaviour.

Phase 3
US Research

Research with 3,000 consumers across the US to assess their attitudes towards privacy and to ascertain how privacy has impacted their buying behaviour.

Could your business use privacy as a market differentiator?

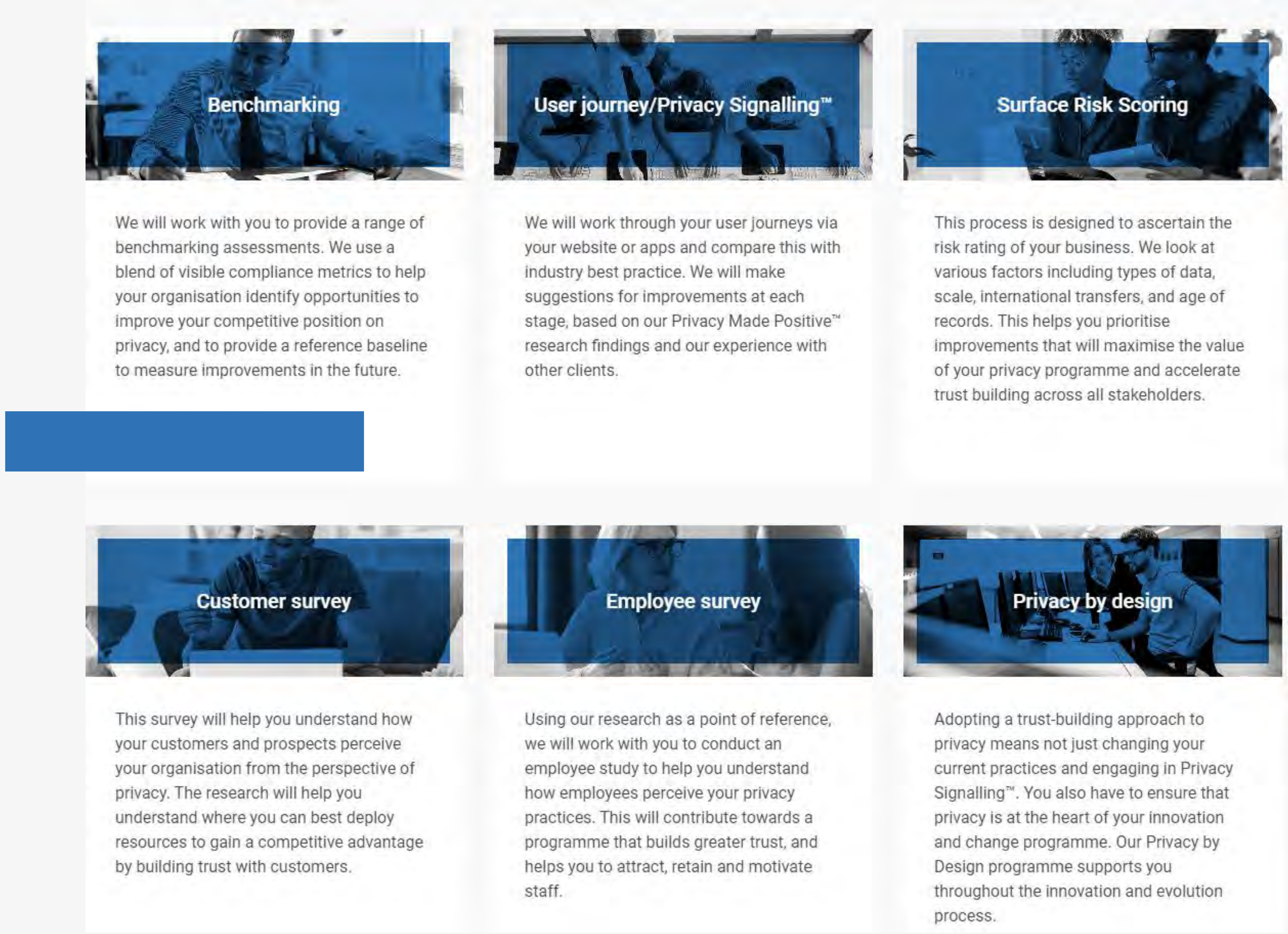
Visit **www.privacymadepositive.com** to find out more.

Privacy Made Positive® toolkit

With our toolkit, we'll help you deliver and embed privacy as a competitive advantage meaning your business benefits are maintained over time.

We've created a practical programme that delivers effective privacy for all your stakeholders.

The tools we offer can be employed as a full end-to-end package or stand-alone components.



Benchmarking

We will work with you to provide a range of benchmarking assessments. We use a blend of visible compliance metrics to help your organisation identify opportunities to improve your competitive position on privacy, and to provide a reference baseline to measure improvements in the future.

User journey/Privacy Signalling™

We will work through your user journeys via your website or apps and compare this with industry best practice. We will make suggestions for improvements at each stage, based on our Privacy Made Positive™ research findings and our experience with other clients.

Surface Risk Scoring

This process is designed to ascertain the risk rating of your business. We look at various factors including types of data, scale, international transfers, and age of records. This helps you prioritise improvements that will maximise the value of your privacy programme and accelerate trust building across all stakeholders.

Customer survey

This survey will help you understand how your customers and prospects perceive your organisation from the perspective of privacy. The research will help you understand where you can best deploy resources to gain a competitive advantage by building trust with customers.

Employee survey

Using our research as a point of reference, we will work with you to conduct an employee study to help you understand how employees perceive your privacy practices. This will contribute towards a programme that builds greater trust, and helps you to attract, retain and motivate staff.

Privacy by design

Adopting a trust-building approach to privacy means not just changing your current practices and engaging in Privacy Signalling™. You also have to ensure that privacy is at the heart of your innovation and change programme. Our Privacy by Design programme supports you throughout the innovation and evolution process.

Client Case Studies

Sagicor

Overview: Large Caribbean financial institution with a 179-year history and strong reputation for customer service excellence, operating in 22 countries across the US, Latin America and the Caribbean.

Objective: Data privacy review to identify any aspects of privacy non-conformity.

Solution: Securys conducted a comprehensive data privacy review across the Caribbean-based operations. The review considered both local and extraterritorial privacy and provided a comprehensive analysis of privacy non-conformity.

Our risk-driven approach, using our proprietary Surface Risk Scoring ™ system ensured a focus on the highest risk areas meaning risk mitigation ran in parallel with continuing discovery, documentation and reporting.

Securys continues to work across Sagicor on multiple operational privacy initiatives.

ANGLO AMERICAN

Overview: Sector- leading organisation, operating in 27 countries with 100,000 employees. Data subjects include employees, contractors and customers of its luxury retail brands.

Objective: The client wanted to review and enhance its handling of personal data across the organisation to help best protect the interests of all stakeholders including employees, consumers and suppliers as part of its global commitment to safety and security across all its operations.

Solution: Responding to the client's need, Securys implemented and continues to operate a comprehensive privacy operating model and privacy as a service delivery model covering all aspects of privacy across 25 territories around the world. The model incorporates process discovery, risk-scoring, assessment and remediation of existing processes, privacy-by-design programme implementation and operation.

Securys implemented and continues to operate a comprehensive privacy model.

STIFEL

Overview: : **This leading diversified global wealth management and investment banking company wanted a review of data transfers from the UK and EU to the US alongside a thorough and detailed review of employee and customer privacy.**

Objective: Following the Schrems II judgment which invalidated the EU-US Privacy Shield, there was a need to interrogate all transfers to the US. We treated these on a case-by-case basis to fully assess each transfer, considering specifically the mitigation of surveillance risk.

Solution: Securys undertook a thorough and detailed audit of employee and customer privacy across the UK and EMEA. Amongst our other activities, this involved interviewing key personnel and reviewing relevant documentation. This process allowed all transfers to the US to be identified and properly assessed. We provided a summary report that highlighted areas of best practice along with practicable implementable solutions for areas where improvement was required

We continue to work with the privacy office team to provide ongoing support.

Overview: Award-wining UK financial trading company which specialises in electronic market making in equity, FX, fixed income and commodity markets.

Objective: Detailed privacy review of UK operations to highlight areas of risk.

Solution: Working within the UK operations, Securys conducted a high-level data privacy review of its operations in the UK to identify areas of particular risk.

The summary report provided an organisation-wide dashboard with an overall risk score and accompanying narrative including both organisation-wide risk treatment recommendations and broader commentary on the organisation’s overall compliance and security readiness.

BARNES ROFFE LLP
CHARTERED ACCOUNTANTS

Overview: A top 50 accountancy firm in the UK with more than 20 partners and over 150 staff spread across multiple offices in the UK wanted a root-and-branch audit of privacy and cyber-security. The firm prided itself on delivering beyond expectations to its client base of owner-managed businesses and private clients.

Objective: following a breach, the firm needed external advice on risk mitigation and best practice.

Solution: Securys conducted detailed interviews, process mapping and document review using this to compile a data catalogue and RoPa and identified processes requiring DPIA and/or LIA support. We provided a comprehensive report with 90-day and long-term action plans which was presented at a Partner Meeting.

Now engaged to assist with remediation and provide ongoing privacy office function. Retained by Managing Partner.

PacBio

Overview: A market-leading life science technology company, with operations globally approached Securys to undertake a detailed review of their compliance with the GDPR within their European and UK operations. Headquartered in the US, this fast-growing organisation employs over 700 employees and is listed on the Nasdaq.

Objective: Looking at marketing, sales, HR, operations and legal, the organisation wanted an end-to-end review from lead generation to customer management. The scope was broad and included employee and finance data, their IT systems as well as their handling of international data transfers to the US considering the demise of privacy shield.

Solution: The Securys team undertook detailed interviews, process mapping and a review of their policies and procedures and records of processing to identify key areas of risk.

Given the aim of strengthening local data protection, Securys provided a detailed report with a risk dashboard alongside specific remediation actions to address the identified weaknesses. An actions log drove the remediation actions.

De Beers

FOREVERMARK
A DIAMOND IS FOREVER

LIGHTBOX
LABORATORY-GROWN DIAMONDS

Overview: Review of data transfers from China and advice on compliance with new legislation controlling transfers of personal data outside China.

Client objective: review the privacy and operational implications of the restrictions on transferring personal data out of China, implement appropriate privacy controls.

Solution: Securys worked with the customer experience and IT teams to understand the existing systems landscape and the data transfers involved in client relationship management and retail sales, which relied on centralised systems and integration to local communication and sales channels.

Securys then advised on technology requirements for a localised platform and privacy control options which met the need to localise data, to continue to gain centralised insight from transactions and to offer Chinese customers travelling outside China the option of personalised service at any store worldwide. We continue to work with the teams to provide privacy-by-design support for the chosen solution.

ROYAL
OPERA
HOUSE

Overview: This major charitable performing arts venue prides itself on its ranking as one of the world’s busiest theatres. Each year, it stages over 2,000 performances and events and employs in excess of 1,000 permanent members of staff.

Objective: Provide advice and support for GDPR readiness and support their compliance programme going forward. Having worked with Securys in a previous organisation, the CIO recognised the importance of ensuring that the personal data of all its stakeholders whether employees, donors or visitors was processed securely and lawfully.

Solution: Securys provided an experienced DPO team to act for the charity. Only ever a phone call or an email away, the outsourced DPO is on hand to provide the necessary guidance and specialist advice. Tailored to the specific needs of the performing arts venue, the advice provided ranges from handling queries and DSAR requests in a timely manner to keeping their documentation updated, undertaking supplier due-diligence and liaison with the regulator.

Client Testimonials

ANGLO AMERICAN

“

Securys has been invaluable in providing me with scalable resource to review and remediate our legacy processes as well as meet the organisation’s demands as it launches new projects and initiatives that involve personal data.

I have been particularly impressed with the efforts they have made to really understand the organisation and the breadth and complexity of the personal data processing activities taking place. This has led to the wider business seeing them as a valued advisor and business partner.

”

PacBio

Peter Fromen
Chief Commercial Officer, PacBio

“

Securys were key to our getting the perfect picture of where we are with privacy compliance for our UK and EU operations. We welcomed their expert insight and knowledge about global privacy and the emerging privacy landscape in the USA and especially their practical advice about how to navigate multiple jurisdictions for a U.S headquartered organization.

The entire process was very smooth from start to finish. The audit was thorough and efficiently managed. The ensuing report and risk dashboard were invaluable in highlighting our areas of strength as well as pinpointing areas of risk that needed attention. It left us knowing exactly what we needed to do next, and we are confident our stronger privacy position will support our continued growth.

”

Sagicor

Willard Brown, Chief Technology
and Insurance Operations Officer

> “Sagicor Group Jamaica is delighted to have Securys onboard as our Data Protection Partner.
>
> Securys’ collaboration with our team showcases a profound grasp of financial services and a comprehensive knowledge of global and local privacy regulations.
>
> Their practical guidance and support have played a pivotal role in ensuring timely compliance with the Data Protection Act across our extensive Group, effectively safeguarding the data of our diverse stakeholders.”

Sagicor

Ronald Blitstein, EVP and Group Chief Information Officer

> *"Even though GDPR is the global gold standard from a regulatory perspective, the data privacy domain is highly dynamic. Countries outside the European Union may have adopted GDPR's key principles, but most have written important variations into their specific legislation.*
>
> *As a multinational full spectrum financial institution, we must comply with evolving and disparate regulations in 20 markets. Keeping track of the shifting regulatory landscape, separating the "wheat from the chaff", and translating that insight into actionable pragmatic programs of work is where Securys excels. They indeed make "privacy practical," which is good business."*

www.securys.co.uk
www.securys.com.jm
www.securys.eu
www.securys.us

Executive Team

The executive team is supported by a diverse multi-disciplinary team across offices in London, UK and Dublin, Eire.

Ben Rapp

Group Chief Executive

Ben was formerly founder and CEO of Managed Networks, a leading UK managed services provider.

He exited that business in 2018 in a trade sale. Ben had also held a number of non-executive roles, including serving on the boards of TechUk and the BCS.

Ben is a CISSP-ISSMP, CIPP/E, CIPP/US, CIPP/M and an IAPP Fellow in International Privacy (FIP), a BCS Fellow and a Chartered IT Professional.

Sara Newman

Director

Sara has had a number of Senior IT operations and management roles, including IT director for a UK top-25 accountancy firm.

She leads client engagement and on-site audit; she also runs our DPO-as-a-Service practice and shares responsibility for internal talent development and retention.

Sara is a CISA and CIPP/E. She also holds PRINCE2 and ITIL certification.

John Lloyd

Director

John has worked in a wide variety of leadership roles in diverse sectors including media, healthcare and non-profit.

He leads our privacy assessment practice and manages the risk scoring and our consultancy team.

John is a CIPP/E and has a number of sector qualifications in safeguarding and information security.

Contact Details

Ben Rapp

Group Chief Executive

Securys

ben.rapp@securys.co.uk

Contact Details

Junior Darrell

Head of Commercial Operations, Caribbean

Securys Jamaica

Junior.Darrell@securys.com.jm

Contact Details

Andre Palmer

Head of Practice, Caribbean

Securys Jamaica

andre.palmer@securys.com.jm