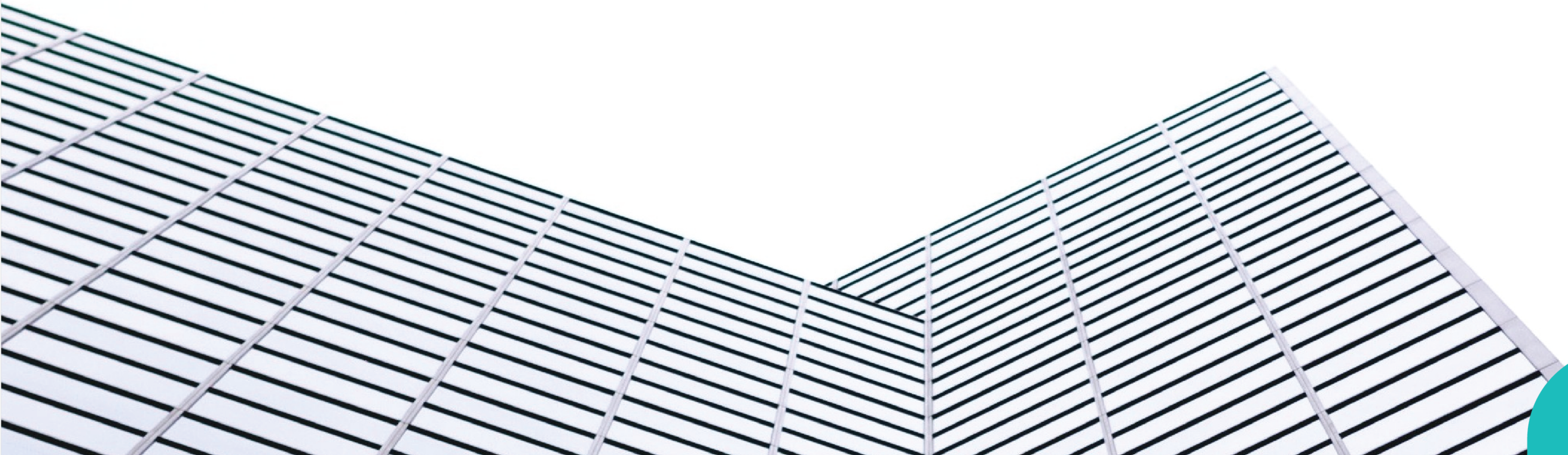
inzalo
EMS

The Evolution of Information Technology in Data Protection and Privacy



April 2021

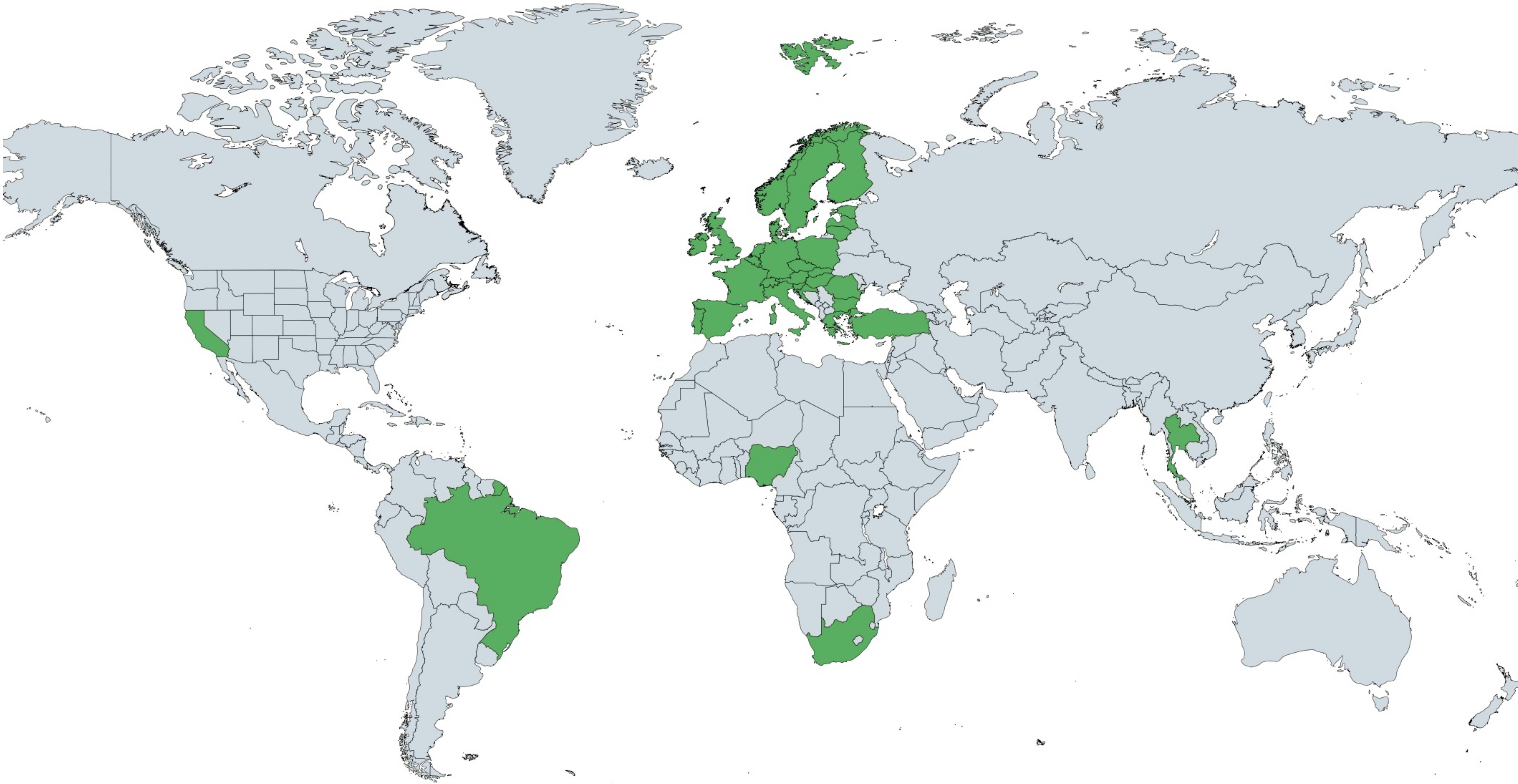
Tai Chesselet
CEO PrivIQ

We provide data protection and privacy compliance management solutions as a cloud-based offering to a broad base of organisations covering various legal regulations worldwide.

Intelligent Compliance, Simply

www.privIQ.com

Our reach - 8 Regulations worldwide, 23% of global economy.



Introduction
To the topic

Data Protection and Privacy is one of the most important topics of the decade as we move to a digital economy.

Gartner

“By 2023, 65% of the world’s population will have its personal information covered under modern privacy regulations, up from 10% today.”

“By 2023, companies that earn and maintain digital trust with customers will see 30% more digital commerce profits than their competitors.”

“By 2024, more than 80% of organizations worldwide will face modern privacy and data protection requirements.”

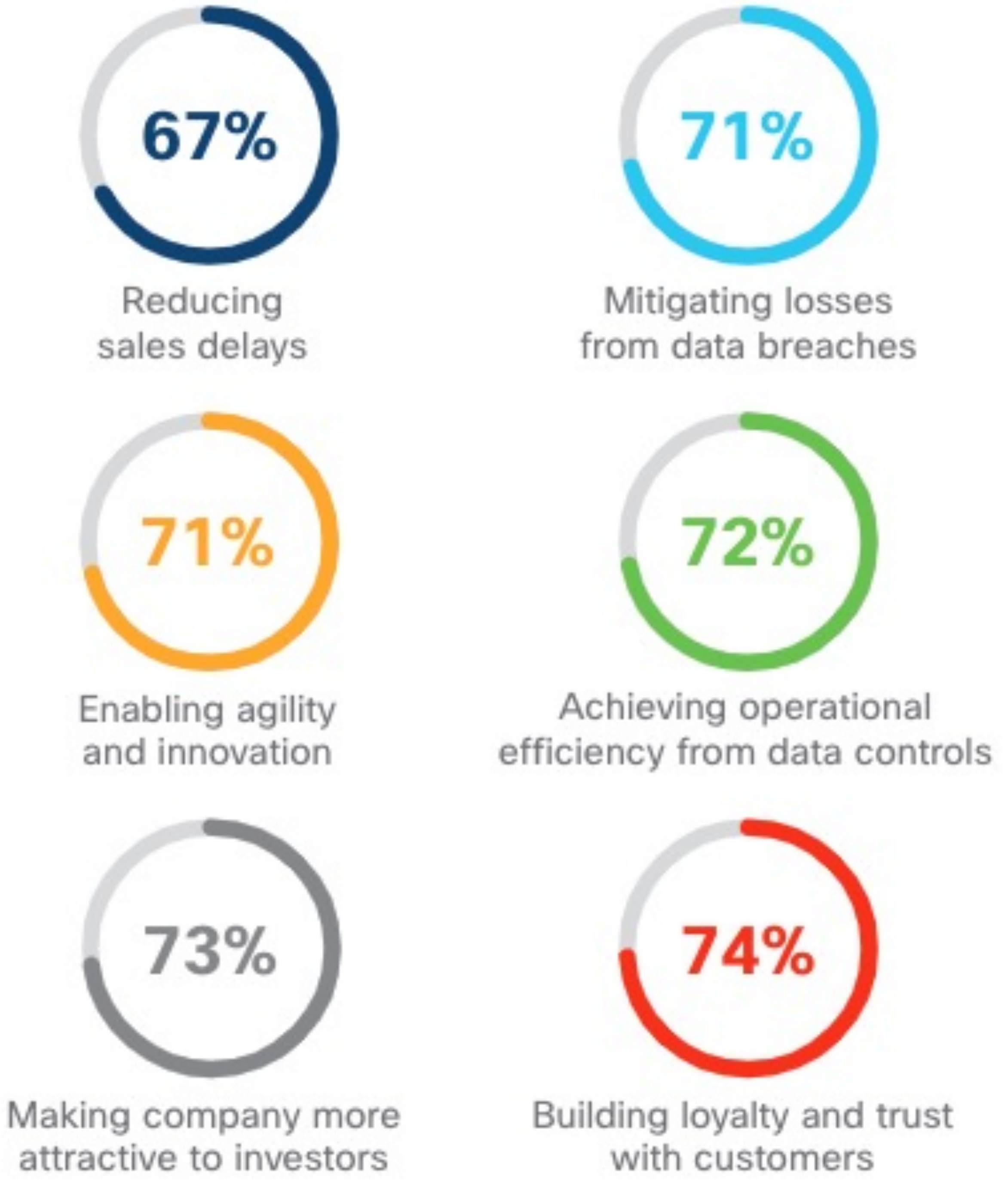
A comprehensive Data Protection and Privacy program will increase your efficiency and trust.

Achieving positive returns on privacy investments

"Most organizations are seeing very positive returns on their privacy investments, and more than 40% are seeing benefits at least twice that of their privacy spend."

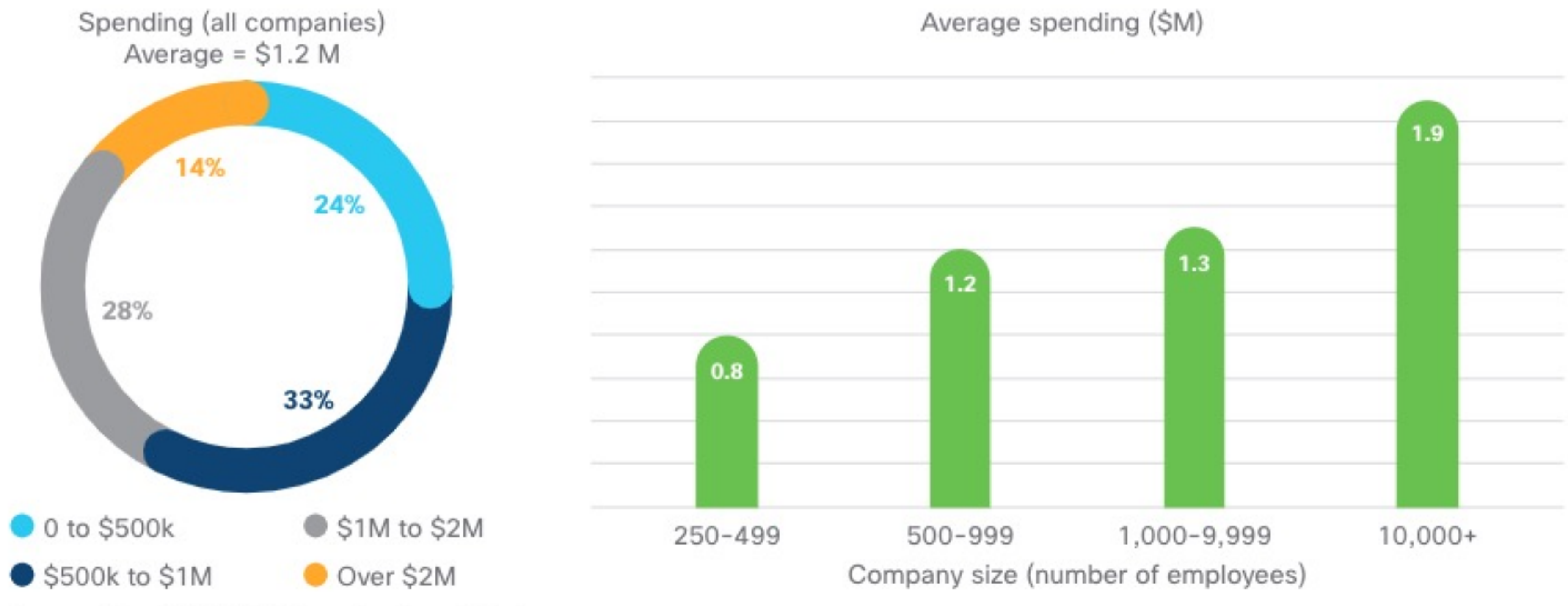
*Cisco Data Privacy Benchmark Study 2020

Business impact of privacy
Percentage of companies getting significant benefits in each area, N=2549



Source: Cisco 2020 Data Privacy Benchmark Study

Annual privacy spending overall and by company size
N=2549



Source: Cisco 2020 Data Privacy Benchmark Study

A quick Reminder, why do we have privacy legislation?

- Personal data belongs to the individual.
- Organisations are entrusted with information on a consensual basis.
- The information is used purely for the purpose it has been given.
- This information must be protected and not put at risk of theft and abuse.
- The Universal declaration of human rights 1948 – declared the right to privacy.
- Organisations using information must respect it.

Why now? – A new philosophy.

- Top of mind topic in the world of hacks, attacks, fake news and cyber-war.
- To remain competitive organisations must take privacy of individuals seriously.
- Organisations are legally required to comply with legislation.
- Large organisations will drive compliance onto smaller ones.
- Personal data of individuals belongs to the them, not the holder of the information
- It can be used for a legitimate purpose with the permission of the individuals
- It must be disposed of when the legitimate purpose has run its course

Problem

Organisations must comply with new laws.

Complex and difficult to understand.

Need a collaborative solution.

Expensive without use of guiding technology.

Requires frequent review to ensure ongoing compliance.

What you need.

privIQ

- Organisation wide compliance
- Demonstrable and proportionate
- Employee awareness and understanding
- Governance policies
- Privacy notices
- Consent management, Direct marketing, HR, IT and security
- Operator contracts – Jointly and severally
- Subject Access request and breach management
- Ongoing review – weekly / quarterly / bi-annual / annual

Managing Risk

MANAGING THE RISKS OF ALL THIS IS KEY

Organisational

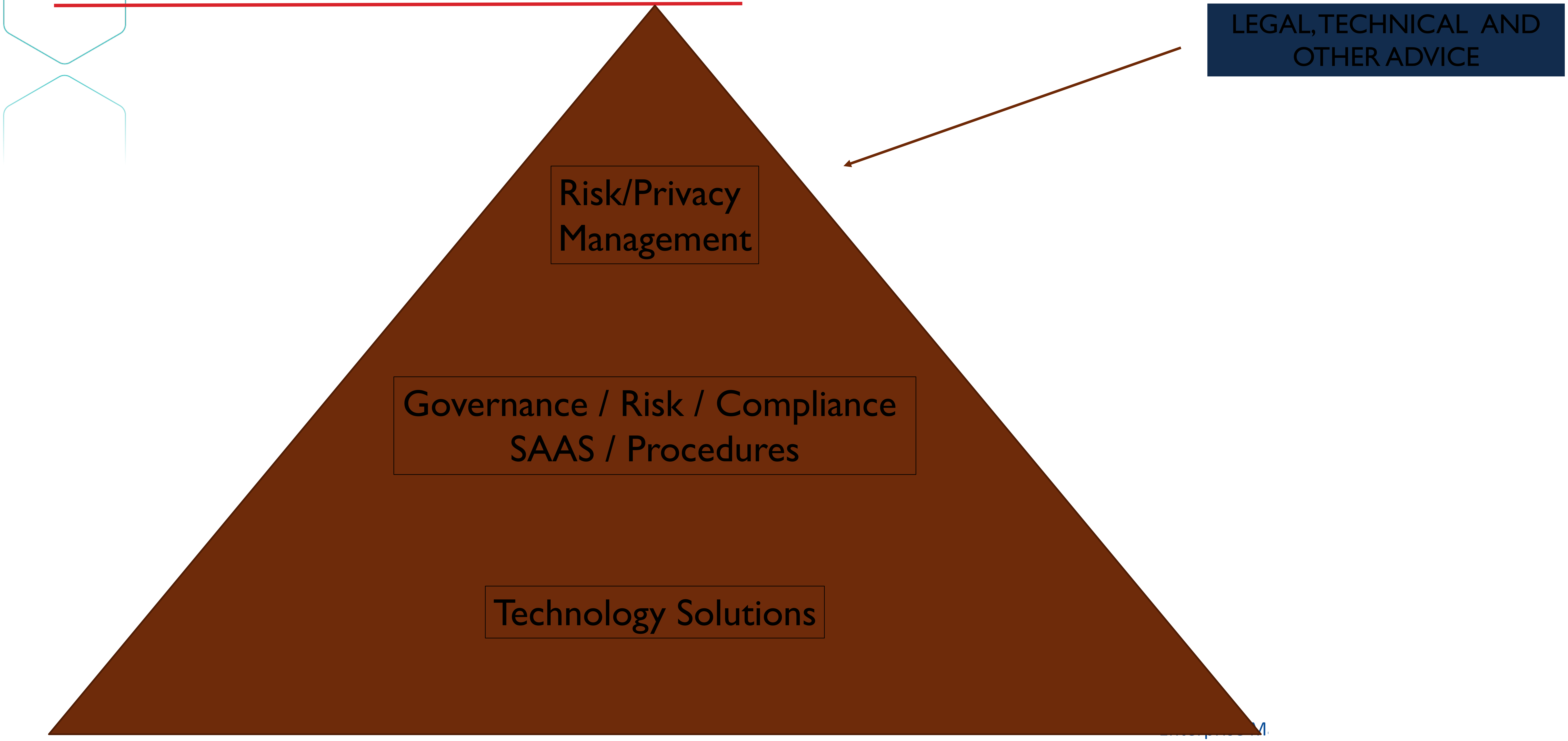
- DPO/GRC/Information officer role
- Employee onboarding
- Amendments to employee policies
- Employee offboarding
- Home security policies
- Governance policies
- Usage policies
- Employee monitoring policies
- Information security
- Privacy statements
- Data Mapping
- Privacy policies
- Reviews of state

Technical

- Telephony Systems.
- Meeting systems.
- Employee equipment
- Server hosting for financial and other systems.
- Cyber-Security services – Network
- VPN's
- Cyber-Security on employee devices
- White listing, black-listing, device control
- Backups, disaster recovery
- Employee monitoring services

DATA PROTECTION ISSUES ARE COMPLEX

Data Protection / Governance Stack



LEGAL, TECHNICAL AND OTHER ADVICE

Risk/Privacy Management

Governance / Risk / Compliance SAAS / Procedures

Technology Solutions

How has Technology Evolved

2 areas
Of Technology

Data Protection and Privacy Program Management solutions

- Manage total Ease of use
- Collaborative
- Dashboards and reports
- Tasks and workflow management

Technological measures

- Backup
- Cyber Security
- Disaster Recover
- Prevention and Mitigation

Technology Measures

Backup	-	Tape to Cloud Databases – replication to another location
Cybersecurity	-	Anti-virus to Increasingly sophisticated using AI, cloud based pattern matching
Disaster recovery	-	RTO - Days to 15 seconds RPO – Previous night to last checkpoint

Data Protection and Privacy Programs

Paper and Excel based to SAAS solutions.

PROPORTIONATE AND DEMONSTRABLE

- Easy to use
- Enables continuity of program
- Allocate tasks
- Obtain status reports dynamically
- All program collateral in one place
- Can be viewed from any location
- Workflows for Access requests, Privacy impact assessments, breach recording.

Home Screen layout

- **Home screen** with all functionality available.

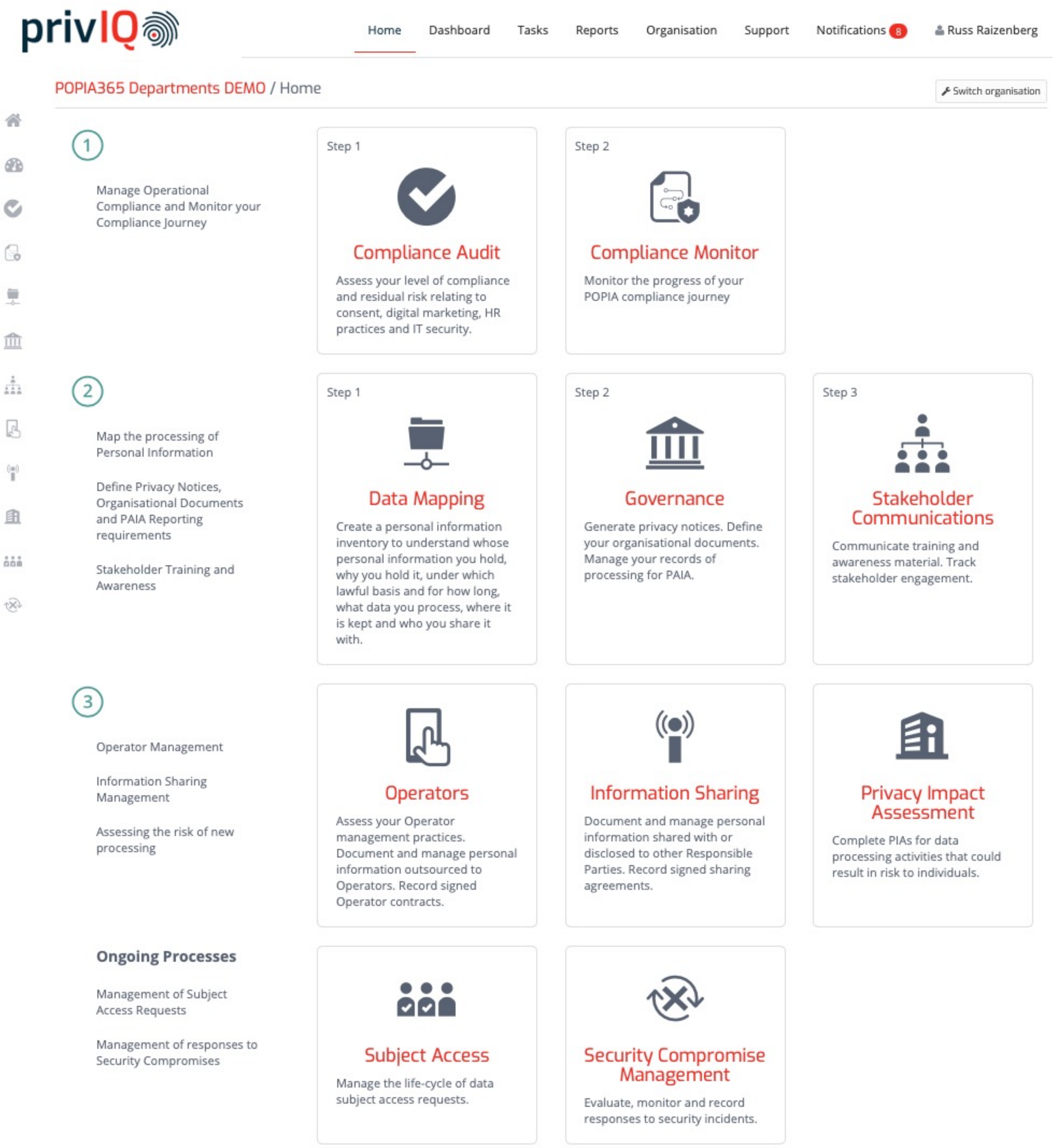
- All text specific to regulation of company.

- Section 1
  - Ongoing compliance reviews.
  - Readiness Assessment of compliance areas.

- Section 2
  - Data Mapping of data subjects, processing purposes and legitimate basis.
  - Governance – Privacy Notices, Governance documents, Document library.
  - Employee training and notification.

- Section 3
  - Operators and data sharing agreements.

- Ongoing processes
  - Data Protection Impact Assessments, Subject access requests and security compromise recording



POPIA365 Departments DEMO / Home

1

Manage Operational Compliance and Monitor your Compliance Journey

Step 1

Compliance Audit

Assess your level of compliance and residual risk relating to consent, digital marketing, HR practices and IT security.

Step 2

Compliance Monitor

Monitor the progress of your POPIA compliance journey

2

Map the processing of Personal Information

Define Privacy Notices, Organisational Documents and PAIA Reporting requirements

Stakeholder Training and Awareness

Step 1

Data Mapping

Create a personal information inventory to understand whose personal information you hold, why you hold it, under which lawful basis and for how long, what data you process, where it is kept and who you share it with.

Step 2

Governance

Generate privacy notices. Define your organisational documents. Manage your records of processing for PAIA.

Step 3

Stakeholder Communications

Communicate training and awareness material. Track stakeholder engagement.

3

Operator Management

Information Sharing Management

Assessing the risk of new processing

Operators

Assess your Operator management practices. Document and manage personal information outsourced to Operators. Record signed Operator contracts.

Information Sharing

Document and manage personal information shared with or disclosed to other Responsible Parties. Record signed sharing agreements.

Privacy Impact Assessment

Complete PIAs for data processing activities that could result in risk to individuals.

Ongoing Processes

Management of Subject Access Requests

Management of responses to Security Compromises

Subject Access

Manage the life-cycle of data subject access requests.

Security Compromise Management

Evaluate, monitor and record responses to security incidents.

POPIA

The eight principles or conditions are as follows:
Principle I – **ACCOUNTABILITY**–the head of the company is ultimately responsible for complying

Principle 2 – **PROCESSING LIMITATION**–usage must be lawful, with the minimal amount of information necessary

Principle 3 – **PURPOSE SPECIFICATION**–collected, used and retained for a specific purpose, related to your organisation's activity

Principle 4 – **FURTHER PROCESSING LIMITATION**–further processing must be compatible with the original purpose for collection

Principle 5 – **INFORMATION QUALITY**–ensure that the personal information is up-to-date, complete and accurate

Principle 6 – **OPENNESS**–things you need to tell the person when you collect their personal information

Principle 7 – **SECURITY SAFEGUARDS**–measures to prevent loss of or unauthorised access to personal information

Principle 8 – **DATA SUBJECT PARTICIPATION**–the information does, after all, belong to someone else –they must be able to access it

In conclusion

- The need to conform internationally has been massively accelerated by worldwide privacy laws.

- To rebuild our economy post-covid we need to be able to participate in the global economy.

- To do so we must manage the data flows and reduce risks wherever possible.

- We all need to ensure we have appropriate risk management, oversight systems and technology measures in place.

- For all of us attending here, there is a great opportunity to be a part of this rebuilding which has positive positive outcomes for all.

Inzalo Enterprise Management Systems

www.inzaloems.co.za