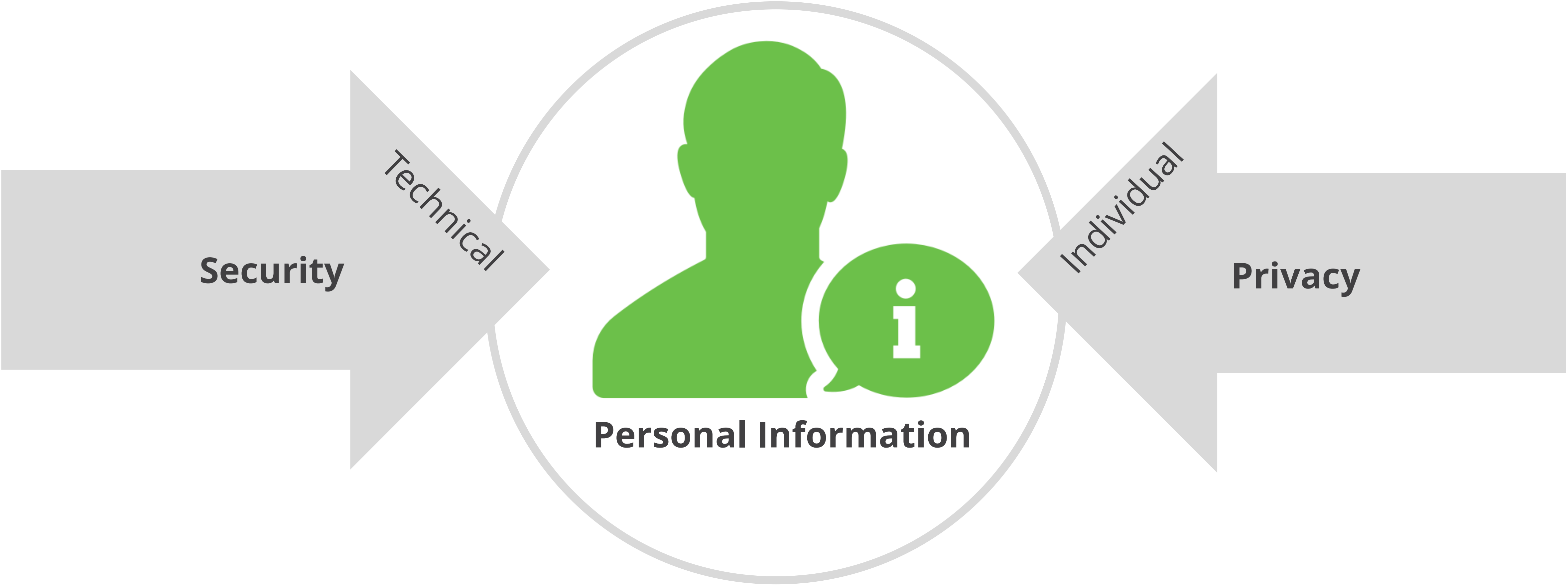
How to Tackle the GDPR: A Typical Privacy and Security Roadmap

Kevin Kiley, VP, OneTrust

OneTrust
Privacy Management Software

Privacy is a Human Issue



Security

Technical

Personal Information

Individual

Privacy

OneTrust

Privacy Management Software

Significantly More Than Just a Privacy Policy Update

> "GDPR requires companies handling EU citizens' data to undertake major operational reform"

Rita Heimes, International Association of Privacy Professionals (IAPP)

Process data for other companies?
This is for you too.

Sample of Ongoing Operational Tasks In GDPR

Legal Basis for Processing	Art. 6
Policy, Notice, Transparency	Art. 13
Data Protection by Design and Default	Art. 25
Data Protection Impact Assessments	Art. 35
Joint Liability with Vendors and Sub-Processors	Art. 28
Data Protection Officer Tasks	Art. 39
Consent Obligations	Art. 7
Cookie, Online Tracking, and Marketing Reform	ePrivacy
72 Hour Data Breach Reporting	Art. 33, 34
Records of Processing Activities	Art. 30
Data Portability and Erasure (Right to be Forgotten)	Art. 17, 20
Subject Access Rights	Ch. 3
International Data Transfers	Ch. 5
Codes of Conduct and Certifications	Art. 40, 42
Security Balancing Risk, State of Art, Cost	Art. 32

OneTrust

Privacy Management Software

Do the Work + Document and Prove It

Legal Basis for Processing
Policy, Notice, Transparency
Data Protection by Design and Default
Data Protection Impact Assessments
Joint Liability with Vendors and Sub-Processors
Data Protection Officer Tasks
Consent Obligations
Cookie, Online Tracking, and Marketing Reform
72 Hour Data Breach Reporting
Records of Processing Activities
Data Portability and Erasure (Right to be Forgotten)
Subject Access Rights
International Data Transfers
Codes of Conduct and Certifications
Security Balancing Risk, State of Art, Cost

x 2

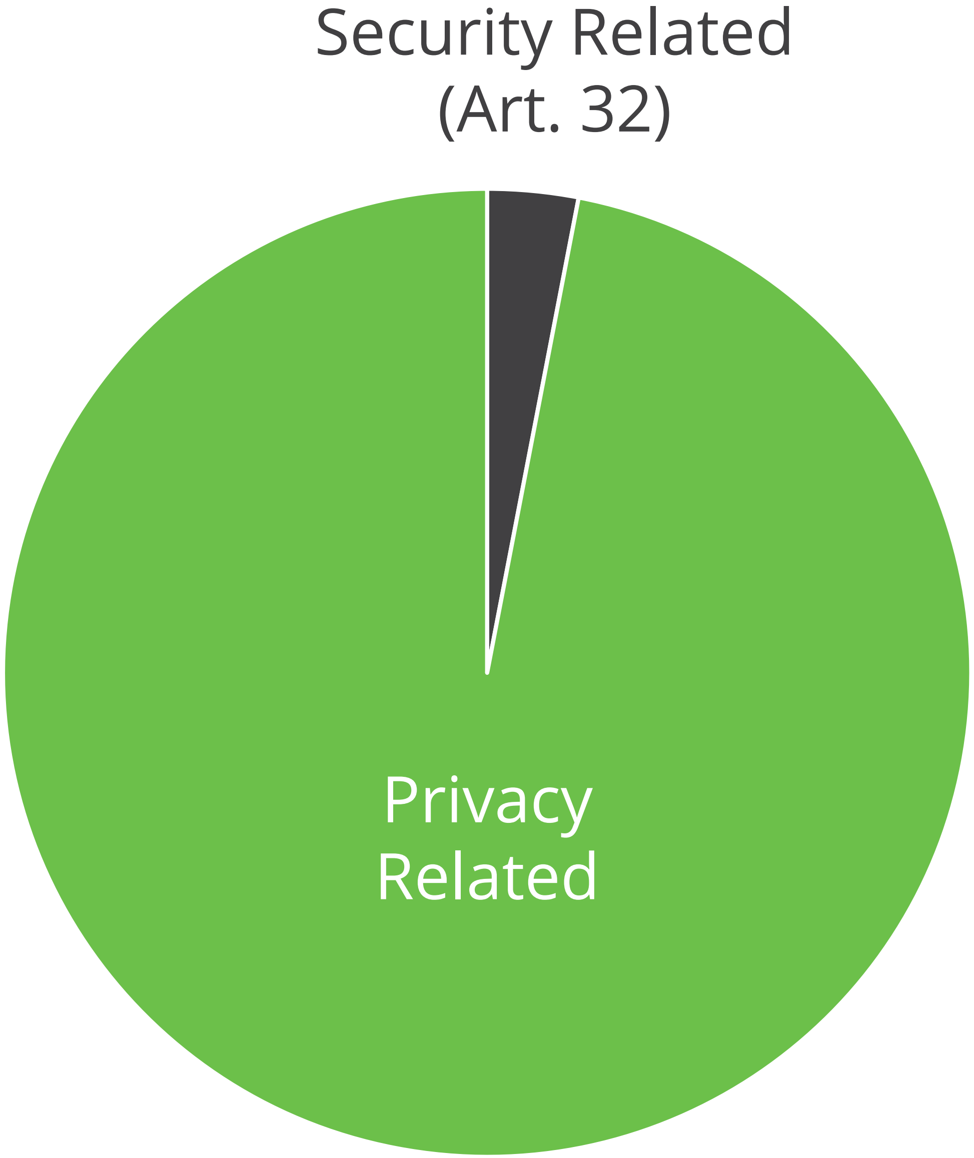
Demonstrate Compliance and Accountability

Art. 5, 24

OneTrust
Privacy Management Software

Breaking Down Requirements in GDPR:

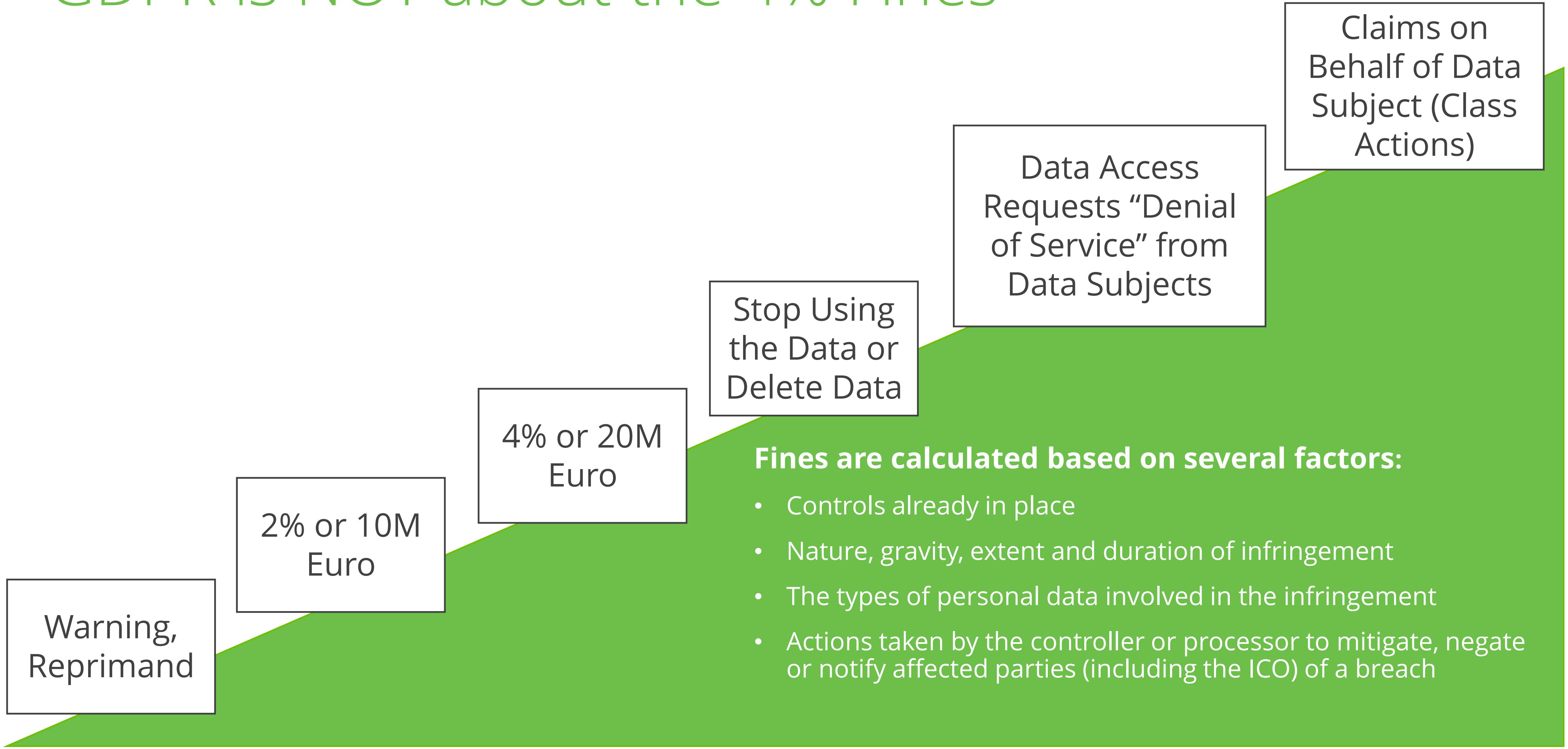
Privacy vs Security



OneTrust

Privacy Management Software

GDPR is NOT about the 4% Fines



Warning, Reprimand

2% or 10M Euro

4% or 20M Euro

Stop Using the Data or Delete Data

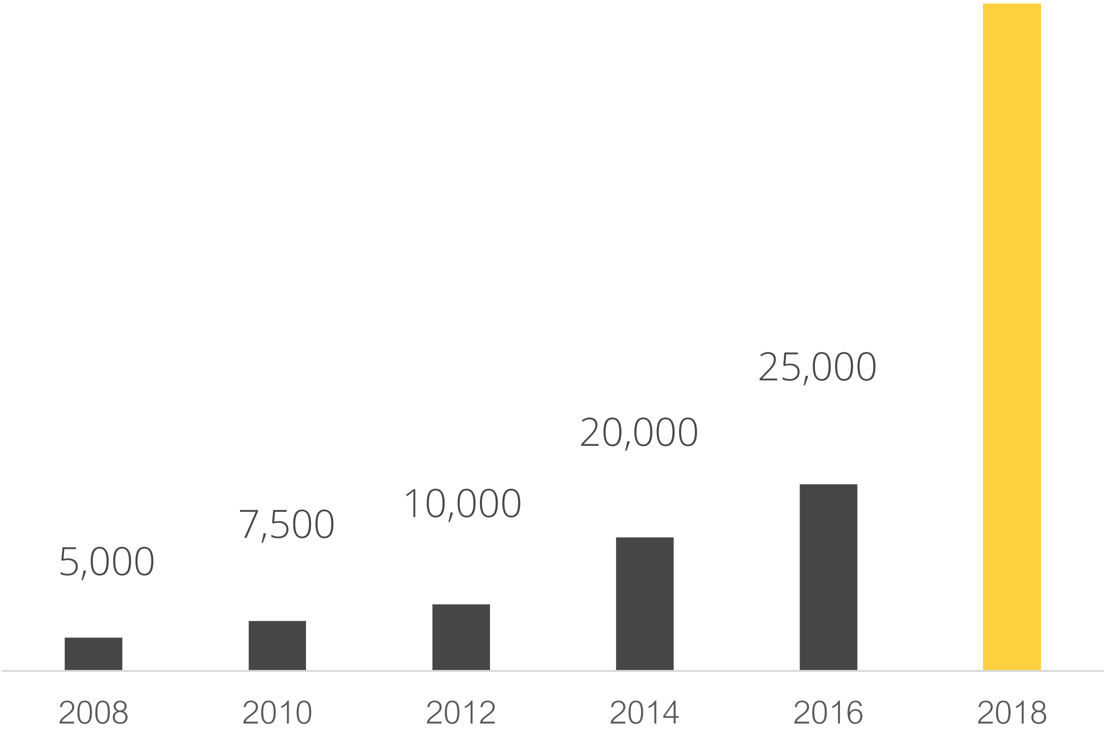
Data Access Requests “Denial of Service” from Data Subjects

Claims on Behalf of Data Subject (Class Actions)

Fines are calculated based on several factors:

- Controls already in place
- Nature, gravity, extent and duration of infringement
- The types of personal data involved in the infringement
- Actions taken by the controller or processor to mitigate, negate or notify affected parties (including the ICO) of a breach

Organizations are Reacting



Study: GDPR's global reach to require at least 75,000 DPOs worldwide

OneTrust
Privacy Management Software

Accountability is Death by a Thousand Cuts

Privacy Policy

Controllers | Processors | Subjects | Consent | Uses | Transfers | Purpose | Retention

Marketing HR Customers Vendors Cloud Government Analytics Support

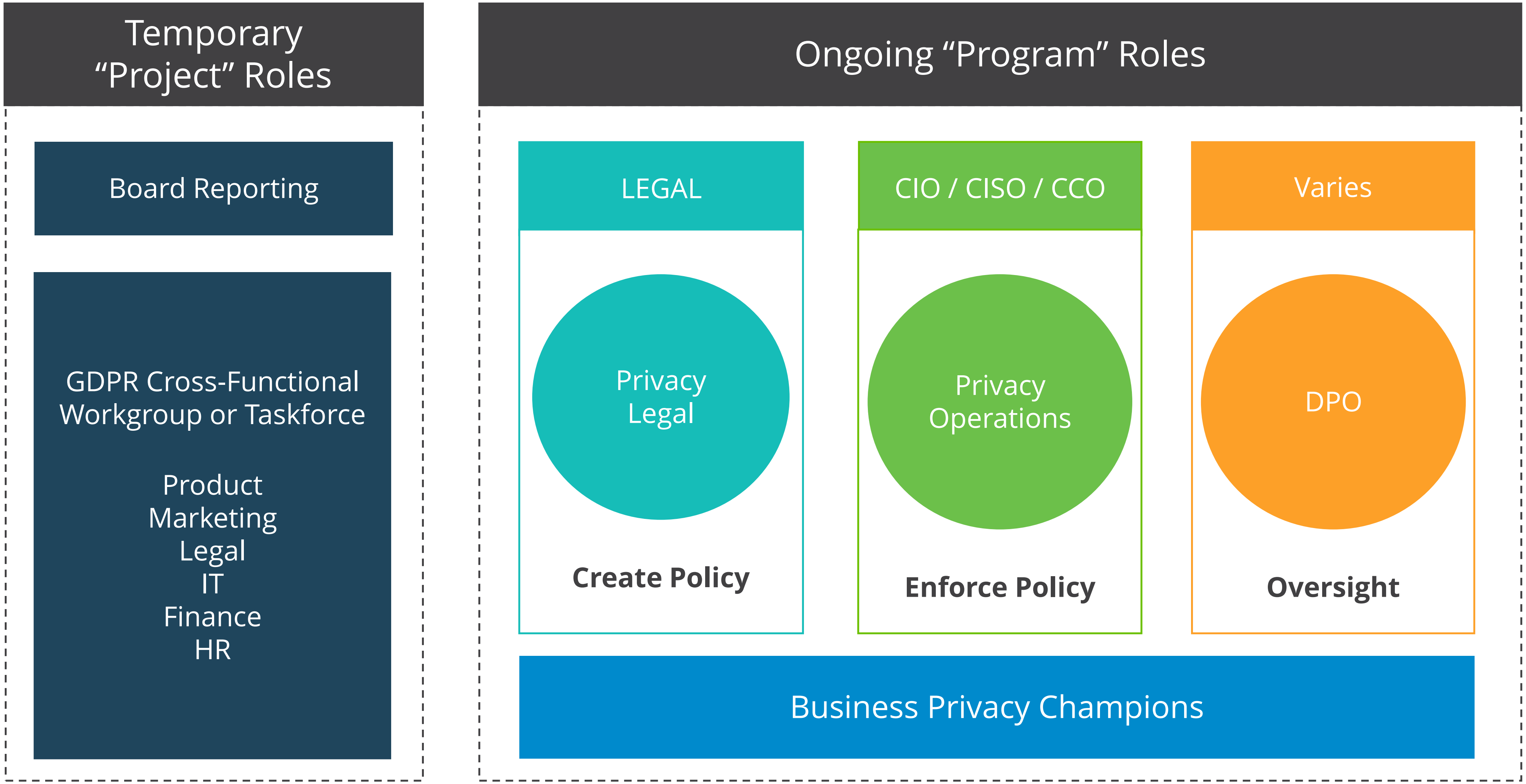
R&D IT Minors Employees M&A Vendors Operations Backups & Testing

Privacy Solutions Needs to be Transformed

Once a Year	→	Continuous, Privacy by Design
Data Entry	→	Strategic consulting
Word and Excel	→	Automated
Burden on business	→	Facilitator of innovation
Incomplete and out of date	→	Complete and real-time
Distraction	→	Reflex

Who is doing the work?

Example of Common Team Structure



Temporary
"Project" Roles

Board Reporting

GDPR Cross-Functional
Workgroup or Taskforce

Product
Marketing
Legal
IT
Finance
HR

Ongoing "Program" Roles

LEGAL

Privacy
Legal

Create Policy

CIO / CISO / CCO

Privacy
Operations

Enforce Policy

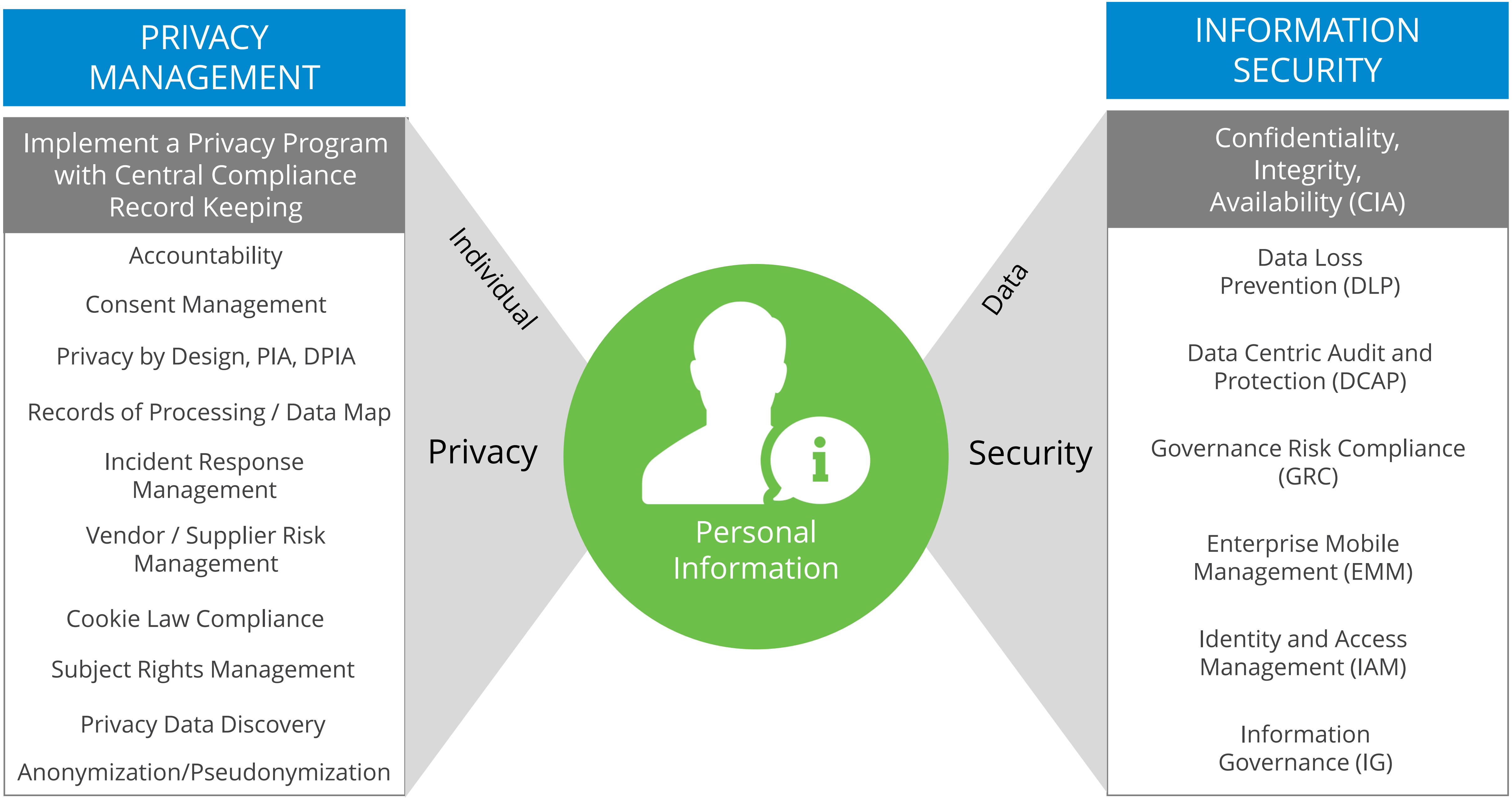
Varies

DPO

Oversight

Business Privacy Champions

OneTrust
Privacy Management Software



PRIVACY MANAGEMENT

Implement a Privacy Program with Central Compliance Record Keeping

Accountability

Consent Management

Privacy by Design, PIA, DPIA

Records of Processing / Data Map

Incident Response Management

Vendor / Supplier Risk Management

Cookie Law Compliance

Subject Rights Management

Privacy Data Discovery

Anonymization/Pseudonymization

INFORMATION SECURITY

Confidentiality, Integrity, Availability (CIA)

Data Loss Prevention (DLP)

Data Centric Audit and Protection (DCAP)

Governance Risk Compliance (GRC)

Enterprise Mobile Management (EMM)

Identity and Access Management (IAM)

Information Governance (IG)

OneTrust

Privacy Management Software

OneTrust GDPR Implementation Software

Readiness & Accountability Tool

Article 5: Principles Relating to Processing of Personal Data

Article 24: Responsibility of the Controller

Centrally document compliance with GDPR

PIA & DPIA Automation

Article 25: Data Protection by Design & Default

Article 35: DPIA

Article 36: Prior Consultation

Review new business projects for privacy risks

Data Mapping Automation

Article 6: Legal Basis for Process

Article 30: Records of Processing

Article 32: Security of Processing

Inventory the business context of your data flows

Website Scanning & Cookie Compliance

Article 7: Conditions for Consent

Article 21: Right to Object

ePrivacy Directive / Draft Reg

Update consent notices on your web properties

Subject Access Request Portal

Articles 12 - 21:
Rights of the Data Subject

Portal to handle the full lifecycle of subject requests

Consent Receipt Management

Articles 7:
Conditions for Consent

Maintain evidence of each individual's consent

Vendor Risk Management

Articles 28, 24 & 29: Responsibilities of Processor & Controller

Article 46: Transfer Subject to Appropriate Safeguards

Properly vet any sub-processors for onward transfers

Incident & Breach Management

Article 33: Notification to Supervisory Authority

Article 34: Notification to Data Subject

Collection and notification workflow for incidents

OneTrust
Privacy Management Software

PrivacyConnect

GDPR Community by OneTrust

Free, Half-Day GDPR Workshops

4.5 CPE Credit Hours

OneTrust Certification Program in Select Cities

Monthly GDPR Webinar Series

Hosted by Top Tier Law Firms & Consultancies

RSVP TODAY: PrivacyConnect.com

2018 WORKSHOP SCHEDULE

Washington DC
Paris
New York
Amsterdam
Frankfurt
Seattle
Dublin
Denver
Vienna
Dubai
Los Angeles
Boston
Berlin
London
Munich
Toronto
Warsaw
Milan
Madrid
Rome
Tallinn
Atlanta
Dallas
Portland
Budapest
Phoenix
Brussels
San Francisco
Chicago
Geneva
Helsinki
Manchester
Stockholm
Tel Aviv
Houston
Columbus
Prague
Belfast

"This was the best GDPR-focused conference I have ever been to. This was not just a high-level look into requirements, but an in-depth educational experience for myself and my colleagues."

OneTrust

Privacy Management Software

OneTrust
Privacy Management Software
General Data Protection Regulation
The Official Text

Visit Our Booth

Product Demos

Full Text GDPR Books

Free Tools & Templates

GDPR Workshops