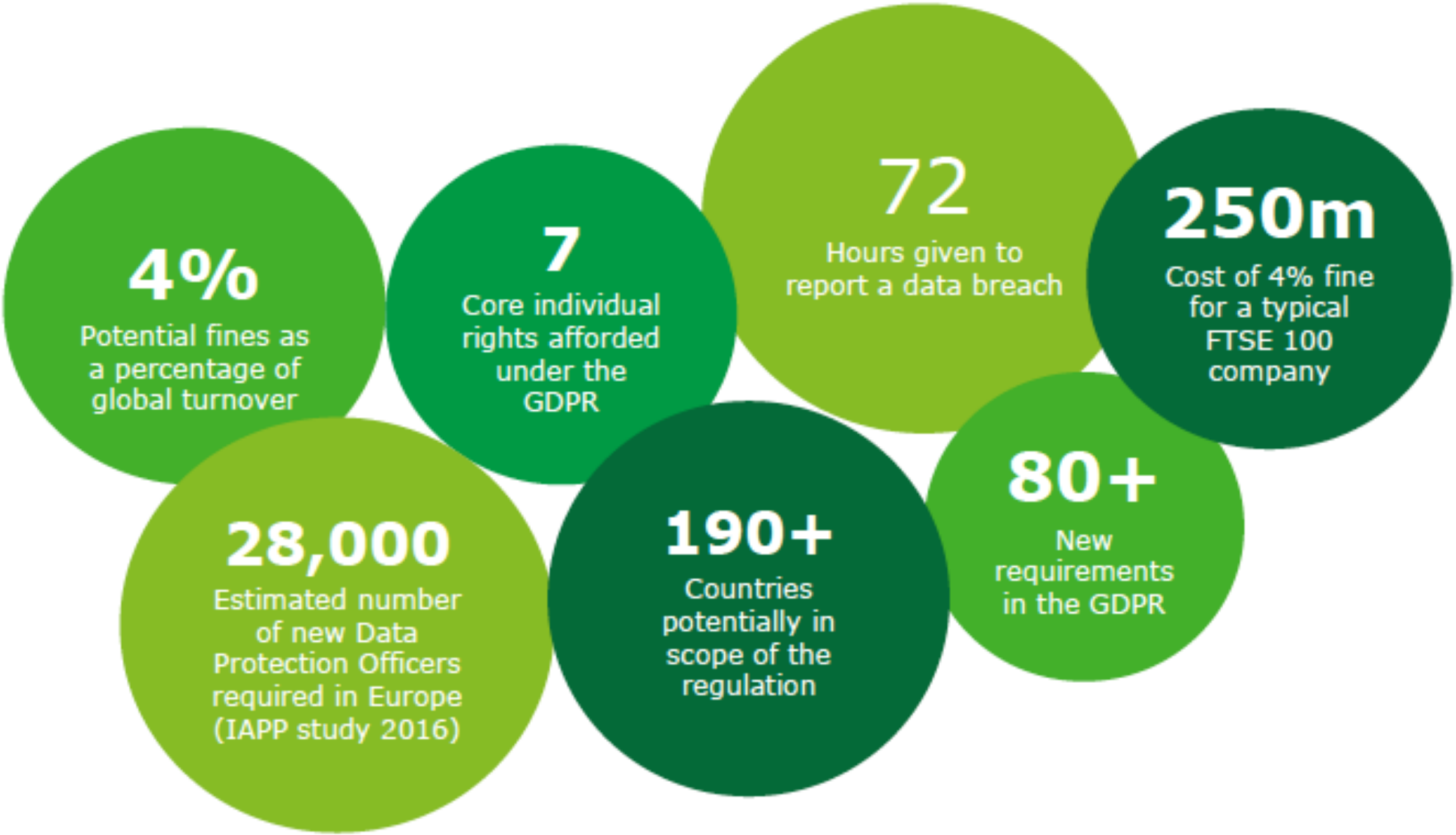

4%
Potential fines as a percentage of global turnover
7
Core individual rights afforded under the GDPR
72
Hours given to report a data breach
250m
Cost of 4% fine for a typical FTSE 100 company
28,000
Estimated number of new Data Protection Officers required in Europe (IAPP study 2016)
190+
Countries potentially in scope of the regulation
80+
New requirements in the GDPR

Layer 1 Strategy

- A strong starting point determining high level direction and risk appetite, upon which the organization builds its privacy organization

Layer 2 Organization

- Enabling effective implementation of the privacy strategy requires a strong and multidisciplinary privacy organizational structure. This covers the structure of the privacy organization as well as the role and position of key players, such as the Data Protection officer. This layer also covers accountability; how to prove compliance?

Layer 3 Policy, process & data

- Partnering with the Business to ensure data is protected, governed, managed and utilized effectively in line with the organization's strategy. Also covers technological challenges such as data access requests, data retention, right to be forgotten, breach notification and international and 3rd party data transfers.

Layer 4 Culture & awareness

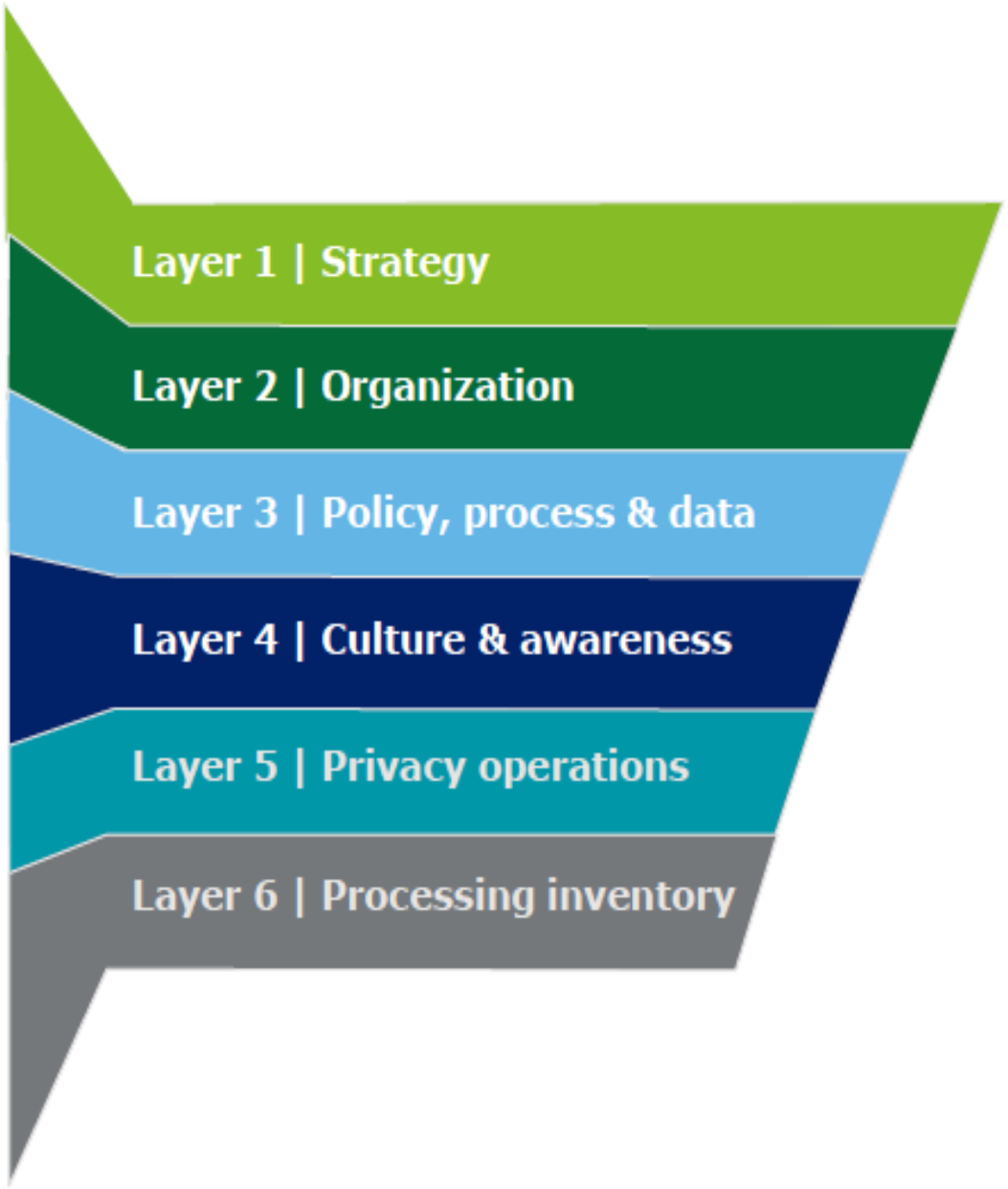
- Creating a high level of organizational awareness on privacy ensures that the organization's employees know and follow the rules.

Layer 5 Privacy operations

- Embedding privacy into the organizations project methodology. This is done by efficient and practical guidance during conception of a new or changed product or service (Privacy by Design) as well as assessing new and existing systems following the established PIA method. Also covers audit guidance and research into privacy seal certification (new option in the GDPR).

Layer 6 Processing inventory

- A processing inventory is a fundamental element of any privacy program, and will be a mandatory requirement following the GDPR;



1. Define	2. Design	3. Implement	4. Operate
• Mobilize stakeholders; • Create buy-in; • Collect baseline information; • Define (key) stakeholders; • Define scope, objectives, stakeholders, timeline and involvement for design phase; • Collect and assess existing documentation; • Create commitment within organization; • Gather necessary approvals.	• Define business requirements; • (Re)design, optimize or harmonize draft deliverables; • (Re)design roles & responsibilities; • Develop implementation plan; • Complete relevant review cycles; • Gather necessary approvals.	• Execute implementation plan; • Piloting new solutions; • Optimize and harmonize solutions; • Implement organizational changes; • Roll out new processes, roles & responsibilities; • Train in the use of new processes and solutions.	• Starting daily operations in newly designed way; • Support of managers and staff to ensure that the new situation is operationalized; • Ensure continuous improvement by using the Plan-Do- Check-Act cycle; • Ensuring hand over to business.

Data Protection Authority (DPA) visit

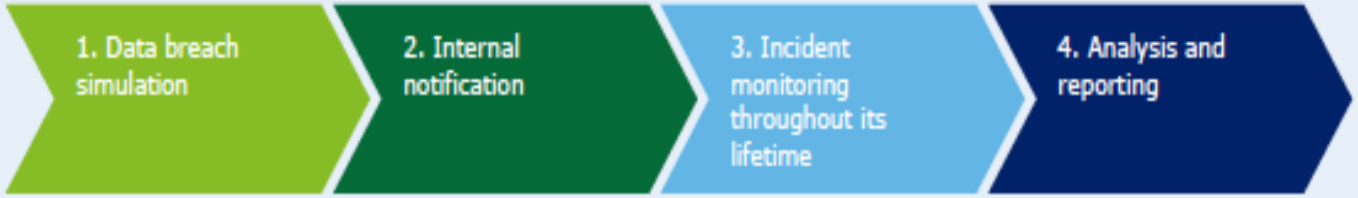
Objective: Simulate a DPA visit to determine resilience of processing activities and measures

Result: Report containing investigation findings, public impact analysis and enforcement action analysis

Data Breach simulation

Objective: Simulate and monitor a personal data breach to determine the status of the current process

Result: Report containing investigation findings, trained employees on personal data breach handling



Public action

Objective: Simulate a DPA visit to determine resilience of processing activities and measures

Result: Report containing investigation findings, public impact analysis and enforcement action analysis