Grant Thornton

Privacy by Design

Think beyond GDPR

May 10, 2018

Speakers

Orus Dearman

Managing Director,
Cyber Risk Advisory

Dhawal Thakker

Senior Manager,
Cyber Risk Advisory

Grant Thornton

Key objectives

Data such as personally identifiable information free flows across organizations.

Silo approach to privacy has proven short of addressing consumer's right to privacy.

Building-in data protection safeguards should happen from the earliest stages.

After completing this session, you will be able to:

- Learn business value drivers for privacy by design
- Understand how to achieve privacy by design
- Complying with GDPR and beyond
- Integrating privacy by design into services

By 2020, the digital universe will contain nearly as many digital bits as there are stars in the physical universe

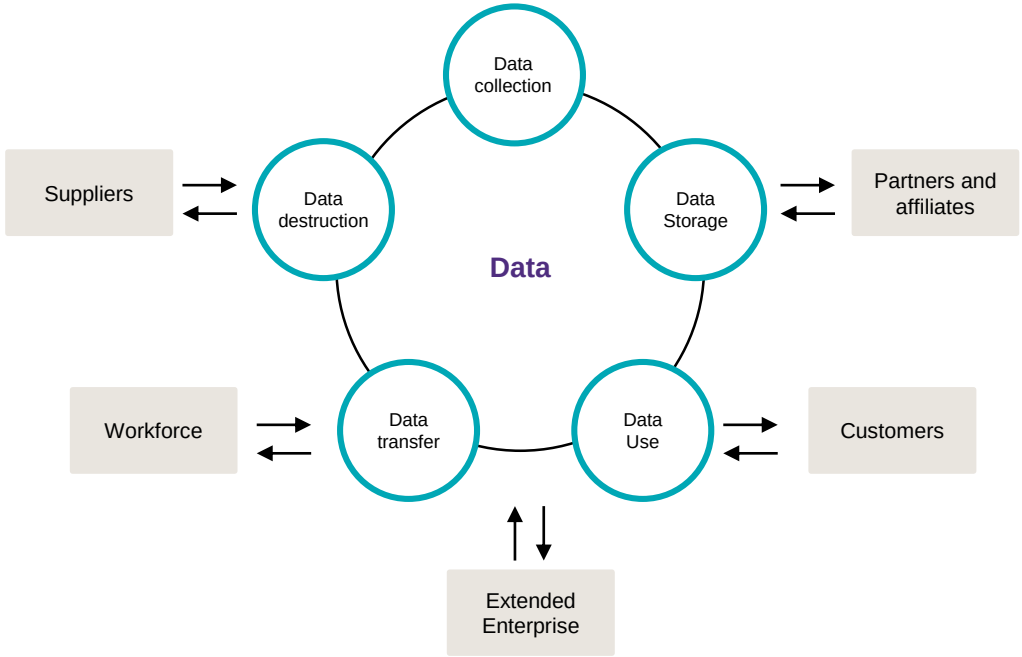
Grant Thornton

Grant Thornton

Market Forces to Privacy and Data Protection

Data is an asset and liability

- Data is emerging as a form of capital in every industry, and also the most coveted asset.
- Organizations are turning into reservoirs and refineries of giant data.
- Free flow of personal information results in a degeneration in what consumers refer to as “privacy friendly” solutions.



Grant Thornton

The struggle for privacy and survival of the protected

Are you prepared:

- What personal data do you hold?
- Whose data is being collected?
- For what purposes is it used?
- How is it secured?
- With whom is it shared?
- How can individuals access it?
- How long is it retained?
- Who within the firm is accountable for it?

Grant Thornton

What is GDPR?

EU General Data Protection Regulation (GDPR) applies to virtually any organization doing business in the EU/EEA

GDPR applies to:

- Organizations based in the EU that process the personal data of natural persons; and
- Organizations that do not have a branch in the EU, but who offer goods and services to individuals residing in the EU and who process the personal data of EU residents.

Accountability is the backbone of GDPR

New rights for individuals	Fair processing notices	Consent	Data Protection Officers	Wider scope	Data Processor obligations	Breach reporting	DPIAs

Key features of GDPR

Grant Thornton

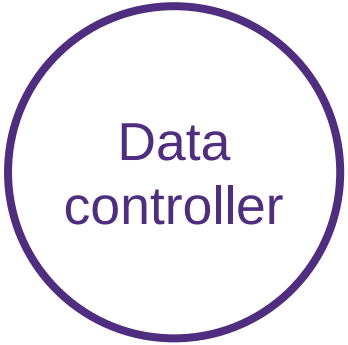
What is personal data?

Personal Data (non-exhaustive list)
Data or combinations of data that can be used to identify an individual.

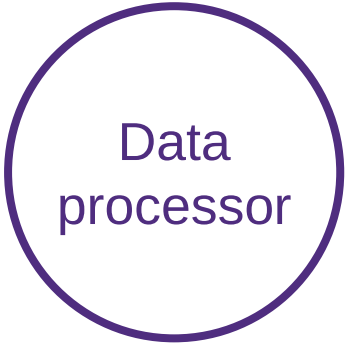
First name	Race	Social network profiles	Gender	Family information	Cookie identifier
National identity number	Nationality			Height	Tax ID number
Login IP	Last name			Place of birth	CCTV
Image	Religion	Home address	Passport number	Email	Bank savings

GDPR personas

- The individual that the information relates to
- The individual has certain rights in respect of the personal data that organizations hold about them

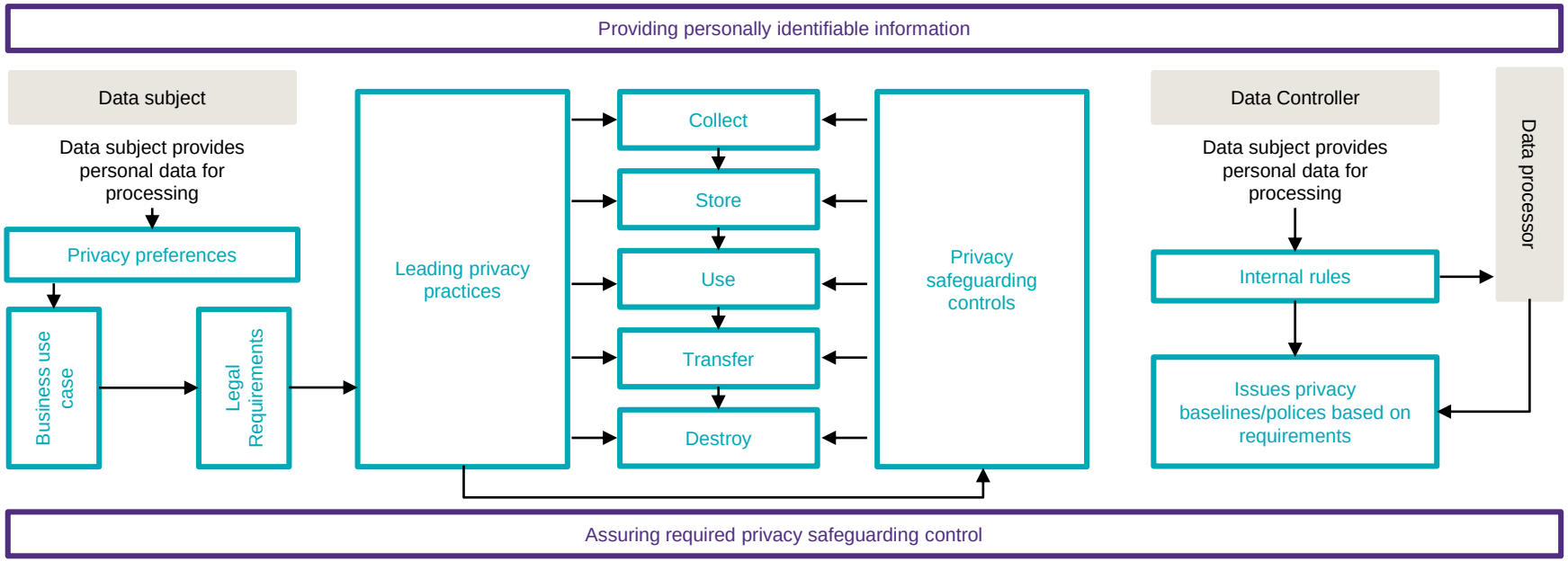


- Determines the purposes for which the data is processed and how
- Responsible for what happens to the data



- Process data on behalf of; or, under the instruction of the data controller

Interaction model between key personas



Poll question

Is your company aware of types of personal data (such as banking information, health information, genetic information etc.) processed by you and your third-parties?

- Yes
- No
- Don’t know

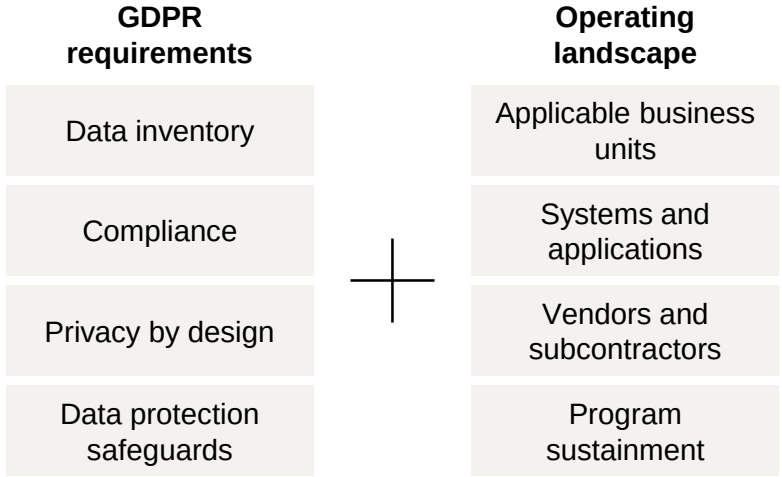
Individual rights

Right to be informed	Right of access		Right to restrict processing	Right to data portability
Right to rectification	Right to erasure		Right to object	Right not to be subject to profiling

What GDPR means to organizations?

As the hard deadline for May 2018 GDPR compliance rapidly approaches, organizations are pushing to achieve compliance. However, focus on one-time compliance over a scalable and strategic approach will result in operational complexities to manage and sustain programs.

- What does GDPR mean to me?
- How do I comply with these requirements?
- May 2018 is here, are we too late?
- Is this a one time exercise? What comes next?
- How can we make this more repeatable?



Grant Thornton

Navigating disparate obligations

Sources

- National, international, state laws
- Regulations, industry guidelines
- Codes of conduct, leading practices
- Cross border requirements

Representative privacy & data protection themes

Consent and choice	Individual participation and access
Customer preference	Cross-border data transfer
Collection limitation	Rights to be forgotten and data portability
Data minimization	Privacy by design
Use, retention and disclosure limitation	Pseudonymization of personal data
Data management	Breach notification
Openness, transparency and notice	Privacy compliance

- Leading practices, industry standards, corporate binding rules, national/ international laws and regulations set the baseline for privacy and data protection frameworks.
- For organizations with globalized operations, it is important to remain current with the requirements of international jurisdictions.
- The common approach adopted across industry is either rationalization or localization of requirements.

Grant Thornton

Grant Thornton

Privacy by Design

Data protection is not just about compliance

Data protection is not only a compliance obligation, but it enables organizations to mitigate risk by identifying data exposure gaps.

Address compliance

Demonstrate alignment to compliance obligations

- Data transfer
- General Data Protection Regulation (GDPR)
- Local privacy laws
- Client contractual obligations

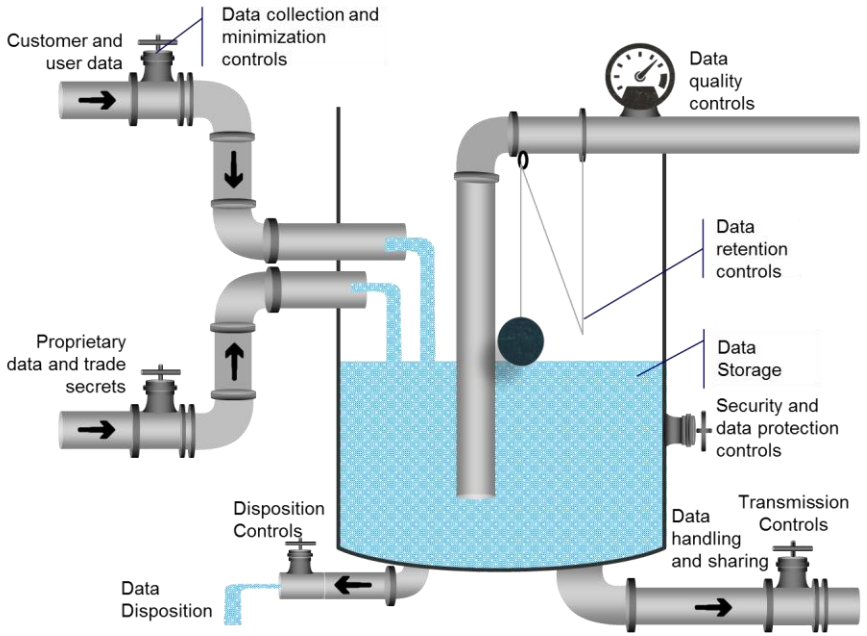
- Data governance
- Data protection
- Data availability
- Incident response
- Breach notification

Manage risk

Make risk based decisions

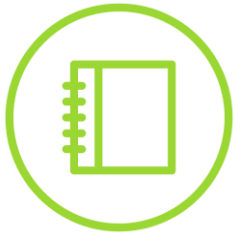
What does it mean to achieve privacy by design

- A typical information system makes quantum connections with neighboring systems and the chain of connections extends to related systems across the organization and its supply chain
- In a real-world scenario, integrating privacy requirements into products/systems/services is not straightforward.
- Privacy, generally is not the primary requirement of a product/system/service build-out and it is not unusual for privacy requirements to conflict with functional requirements.



Grant Thornton

What are the common challenges?



Non-homogeneity of laws and regulations

Uneven playing field created by national and international privacy laws and regulations

Legacy solutions are beyond repair

Legacy solutions are poorly suited to address the emerging class of privacy risks

Disarray due to competing priorities

Multiple stakeholders and interests creates competing priorities of disparate parties

Time-to-market overshadows privacy

Products and solutions are sometimes rushed to market for competitive reasons without thought to privacy

Lack of visibility of data and its flow

Data on defenseless information systems are data waiting to be stolen

Grant Thornton

What is privacy by design?

Privacy by design is an opportunity to:

- build intuitive, user-centric products that embody the organization's commitment to its customers and to data privacy
- proactively plan and integrate privacy principles into the design and implementation of products, services, systems, processes and technologies to enhance privacy protections in the most effective manner

Build and sustain value to customers

Privacy ready features built into product and services

Turn compliance into competitive advantage

Help management make better informed risk decisions

Grant Thornton

Poll question

What is your organization's familiarity with privacy by design before today?

- Very familiar - my organization integrates privacy principles during design of services/ solutions and acquisition of services/ solutions
- Less familiar - my organization is less familiar of privacy by design
- Don’t know

Grant Thornton

Why privacy by design?

Failure to formally integrate privacy

- Identifying privacy flaws after the product or service has launched are more likely to require expensive fixes
- Failing to build and document privacy and security controls into products eliminates the opportunity to mitigate regulatory penalties in the event of a breach
- Ignoring the value that customers place on you for securing their personal data, creates distrust and can damage a company's reputation

Benefits offered by Privacy by design

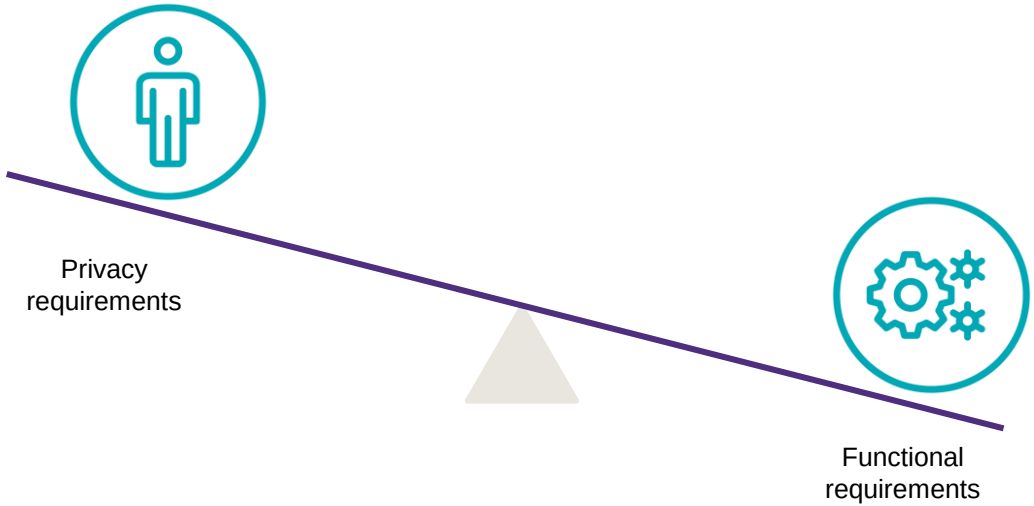
- Identifying and remediating privacy gaps at the early stage of the product development cycle is simpler and/or less costly
- Following the Privacy by Design methodology during the engineering process addresses existing privacy gaps in products and trains engineers to better design future products
- Integrating privacy principles into products helps organizations avoid data breaches, violations of privacy laws, and damage to consumer trust

Grant Thornton

The reality!

Privacy, generally has not been a primary requirement of a product/system/service build-out.

- Tangible engineering strategies utilizing privacy by design still remain unclear for many organizations.
- Hence, the trade-off between privacy and business value should be reviewed sensibly (via risk based approach) within the constraints of agreed upon purposes



Grant Thornton

Grant Thornton

Piecing the Puzzle

Integrating privacy into your organization

The genesis of privacy is to protect users' rights and their freedom, which is why privacy by design is a stride towards consumer centric design. The core building blocks are:

Data privacy governance

Business unit	Lines of business	Divisions/Regions	Functions	Extended organization

Incorporating privacy into business processes and client services

Fairness and transparency

Fair processing of data and transparency of data processing to individuals.

Purpose Limitation

Collection of personal data for a specific, explicit and legitimate purpose.

Data Minimization

Collection and processing of personal data to the extent that is limited to what is necessary.

Data Accuracy

Collection and processing of personal data to the extent that is accurate and complete.

Individual Rights

Individuals must have the opportunity to exercise legal rights in relation to their personal data.

Storage Limitation

Retain personal data for as long as it is needed for the purpose for which it was collected.

Data Security

Protection of personal data by appropriate security measures.

Accountability

Demonstrate compliance with the data protection laws and data protection principles.

Grant Thornton

Poll question

How would you characterize the privacy program operation within your company?

- Privacy capabilities are well understood and appreciated by the business
- Privacy principles are vaguely understood with limited participation and buy-in by the business
- Minimal visibility of privacy, limited to no visibility of personal information processed or stored by the company or the third parties
- Don't know

Grant Thornton

What are the leading practices to refer to?

Leading practices and guidance from industry standards can be leveraged as baselines when building your privacy program. Remember, no standards are plug and play; it has to be tailored to suit your operations and culture.

Provide practical guidance and interpretative assistance on GDPR obligations

Provide privacy framework and describes privacy safeguarding considerations

Provide practices for personally identifiable information protection

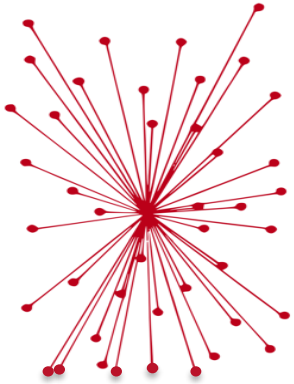
Provide guidelines for privacy impact assessment

Describes principles relating to management of records regardless of structure or form

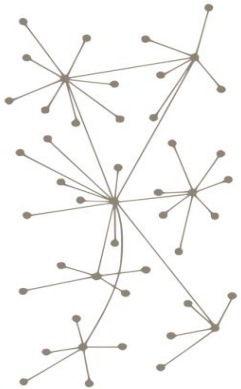
Data inconsistencies

Vast majority of organizations use distributed, decentralized network. Unless the data lineages are clearly established it is hard to protect data and apply reasonable controls. if the data reflects inconsistently across different sources, this can affect decision-making in several ways.

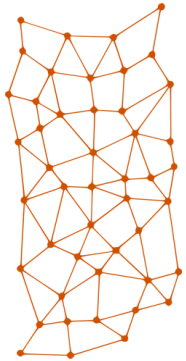
Centralized



Decentralized



Distributed



Grant Thornton

Changing how we think and act about data protection

Minimum expectations to kick start privacy by design journey

Data governance	Data architecture	Data minimization	Data integrity	Data encryption
Without effective data governance, data protection is uncontrolled and can be compromised	Is a framework that outlines what data exists in which locations and how it moves through the organization's network	Entails that any data that is collected and processed should only be retained for as long as necessary	Refers to the ensured completeness, accuracy and consistency of data across all sources	Practice of storing information in such a way that it is only accessible to those that is intended to access.

Grant Thornton

Where to start?

Key privacy and data protection objectives

Data governance | **Data architecture** | **Data minimization** | **Data integrity** | **Data encryption**

Ways to get started..

Inventory and prioritize business processes based on inherent privacy risks

Use GDPR as a framework to rationalize privacy mandates and address other overlapping obligations

Embed privacy requirements into design through Data Protection Impact Assessments (DPIA) and remediation

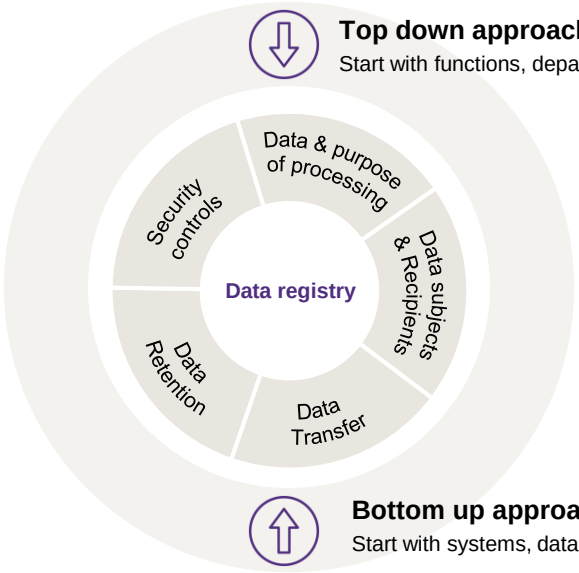
Grant Thornton

1. Records of processing

Know your processing activities and underlying data elements.

Knowing the unknowns:

- Business owner
- Process and system/application owner
- Categories of personal data collected
- Data subjects (e.g., employees, customers)
- Lawful grounds for data processing
- Volumes of data
- Where data is stored (location)
- With which internal systems/applications is data shared
- With which external third parties data is shared
- Retention period
- Who has access to the data



Grant Thornton

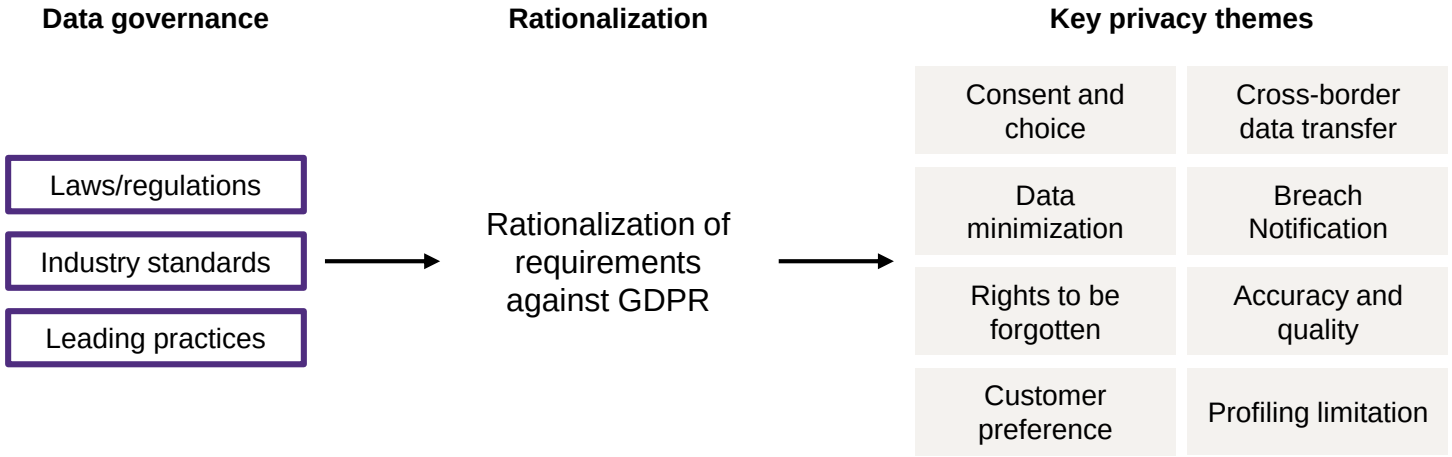
Poll question

Does your organization have a clear understanding of the business processes, applications and systems that process and/ or store personal information?

- Strong yes (80% - 100% confidence)
- Moderate yes (50% - 80% confidence)
- No

2. Rationalize privacy mandates

The approach streamlines the convergences between disparate framework, while at the same time preserves the uniqueness/ outlier requirements.



3. Data Protection Impact Assessment

DPIA provides an opportunity to proactively plan and integrate privacy principles into the design and implementation of products, services, systems, processes, and technologies.

Business processing background

- Processing meta data collection
- Purpose
- Data type
- Risk of harm
- Data Volume
- Activity Type

Assessment of processing

- Minimization
- Accuracy of records
- Record retention
- Basis of processing

Data subject rights

- Data subjects' right to information
- Right to object
- Right of access
- Right to restrict processing, data portability, erasure and rectification

Data transfer mechanisms

- Data transfer mechanisms and controls

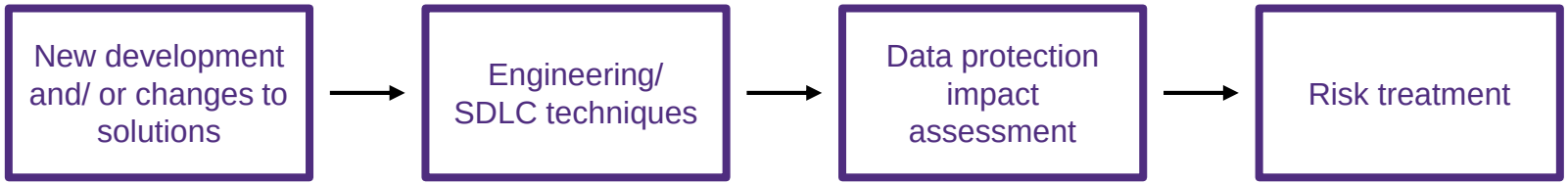
Risk management

- Recording of the risks, controls, and decision

Grant Thornton

3. Integrating DPIA into SDLC (contd.)

DPIA can be a powerful tool in enabling privacy and data protection controls for new services and solutions.



- New solution build or acquisition
- Changes to solutions
- Enhancing functionality

- Waterfall model
- Agile development
- Spiral method
- Consent automation

- How PII is collected and processed
- For what purpose PII is processed
- How PII will be managed
- What is the PII retention and disposal requirement
- How will PII processors protect PII

- Encryption
- Multi-factor Authentication
- Access Control
- Contractual terms and conditions

Poll question

Has your company attempted to perform a data protection impact assessment on critical processing activities, systems and applications during design and/or acquisition of services or solutions?

- Yes
- No
- Don’t know

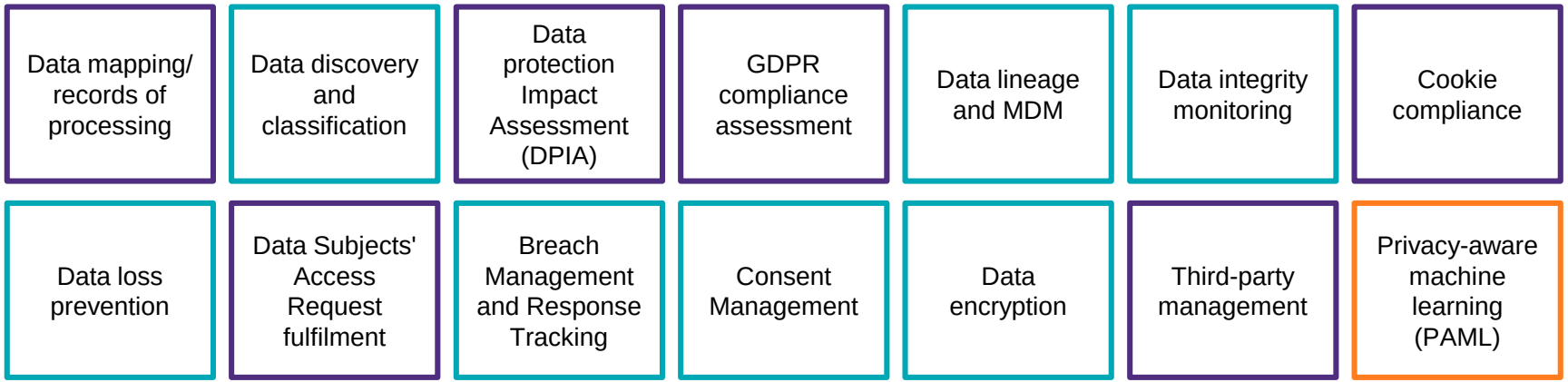
Shared synergies

Privacy does not operate in a vacuum – understanding the unified values and the shared synergies is key to sustain the privacy program and to make privacy stick.

Records of processing	Rationalized privacy mandates	DPIA
Records of processing is a common consumable that is leveraged by privacy, information security, asset management, resilience and contingency planning teams.	Rationalized privacy mandates are enforced as compliance policies and requirements and leveraged by the privacy, compliance, information security and operations teams.	DPIA has a close association with SDLC and system engineering practices and enforced during product or service acquisitions, system developments.

GDPR automation use cases

Organization's business challenges drive the need for automation cases. Below is a non-exhaustive list of GDPR automation use cases:



Grant Thornton

What AI can offer to GDPR?

Data Discovery and Classification

AI applications can accurately discover, classify and protect all types of (sensitive) personal data- structured and unstructured

Compliance Reporting and Dashboards

AI capabilities can be deployed for continuous readiness monitoring, principle- and/or risk-based dashboards, and targeted summary reports for business risk managers and data protection officers (DPOs)

Servicing Subject Access Requests

Natural language processing (NLP) can be deployed to deal with high-frequency customer interactions (for example, in the context of answering subject access requests [SARs]

Privacy Preservation in Analytics

AI applications can enable de-identification of personal data and, subsequently, enable advanced analytics

AI capabilities might add to the risk of re-identification. AI-based decision making is often hard to explain and can have implications with adherence to Article 22 of the GDPR (relating to decision based solely on automated processing).

Grant Thornton

Where is industry with respect to GDPR?

52%

companies expect to be compliant on or before the May 25 deadline

40%

companies expect to be compliant after the deadline

8%

companies were not sure when they will achieve compliance

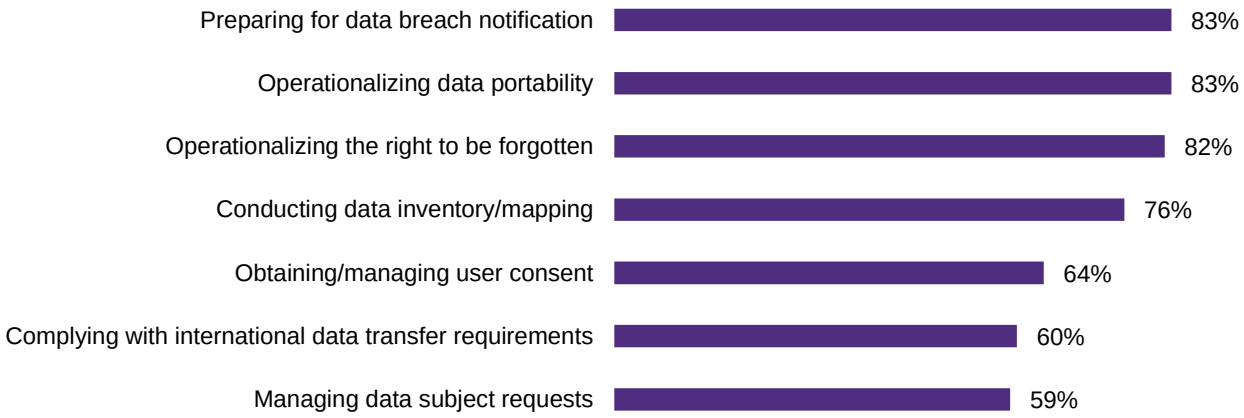
What are the barriers to GDPR compliance?

Source: The Race to GDPR: A study of Companies in the United State & Europe; Ponemon Institute, April

Grant Thornton

Where is industry with respect to GDPR?

What are the barriers to GDPR compliance?



Source: The Race to GDPR: A study of Companies in the United State & Europe; Ponemon Institute, April

Commonly debated topics

GDPR has spurred a lot of debate and discussions when it comes to implementation – the common debated items are reviewed here.

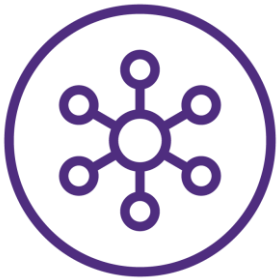
How do you manage records of processing?	Does your plan address processes that really matter – crown jewels?	Have you purged data in-sync with retention thresholds?	Which automation use cases are likely to drive value?	How do you manage user preferences?

Spiraling effects flashpoints

- Records of processing versus asset catalog
- DPIA versus risk assessments
- Data retention versus data disposition
- When is consent needed and when not needed?

Debate 1

Records of processing versus asset catalog



How do the records of processing (RoP) relate to or differ from configuration items in a configuration management database (CMDB)?

Considerations

RoP focus on processing activities related to personal data whereas CMDBs are broader in scope

RoP convey more details relating to processing activities (such as purpose of processing, lawful basis etc.)

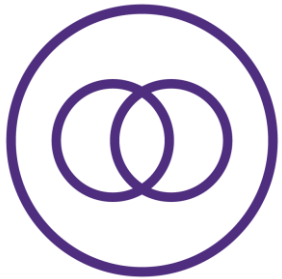
A trustworthy CMDB can be a good starting point for standing-up RoP

Synchronize and standardize CMDB and RoP where possible with your GRC program

Grant Thornton

Debate 2

DPIA versus risk assessments



Is data protection impact assessment (DPIA) still required when organizations routinely perform standard system risk assessments?

Considerations

DPIA is a statutory requirement under GDPR

The risks to rights and freedoms of individuals is the focus of DPIAs; not as much for standard risk assessments

DPIA has a focused scope in discerning the safeguards involved in personal data processing

Leverage the system risk assessment as an intake point for DPIA

Grant Thornton

Debate 3

Data retention versus data disposition

How long should you retain data?

Considerations

Personal data should be retained only so long as necessary to fulfill business and regulatory needs

Prolonged retention is allowed only on selected cases, when the data is anonymized

Shared systems may support multiple jurisdictions and hence bound to align to varying data retention periods

Consider the data schema and organization before purging data

Grant Thornton

Debate 4

When is consent needed and when is it not needed?

On what occasions an individuals' consent is required?

Considerations

A lawful basis should be established when processing individuals' data

Physical posters, billboards, radio advertisements, and other public advertisements does not require consent

Targeted marketing advertisements and emails require explicit user consent

Understand type of data being processed, purpose of processing, and relationship with data subject

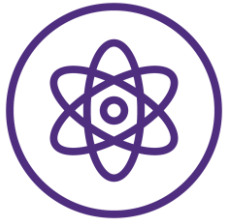
Grant Thornton

Keep your fundamentals right

An organization has to grow its own muscles to get stronger on privacy by design league – which is enabled through the Governance, Process and Technology components.

People

- Governance and operating model
- Data privacy and protection strategy
- Privacy policies and standards



Process

- Data registry and sustainment
- Data protection impact assessment
- Privacy and data protection compliance review

Technology

- Focused privacy automation use cases (data registry, DPIA, privacy compliance)
- Integration with GRC

Grant Thornton

- The genesis of privacy is to protect users' rights and their freedom; which is why, privacy by design is a stride towards consumer-centric design.
- Consumer-centric design does not operate in a "building products by techies for techies" manner; instead, it focuses on transparent and trustworthy design.

Do you know about data privacy day?

Respecting privacy, safeguarding data, enabling trust

www.grantthornton.com

twitter.com/GrantThorntonUS

linkd.in/GrantThorntonUS

Grant Thornton