Technology-enabled
business transformation.

Is your business ready for the next data revolution?

Preparing your organisation for GDPR and beyond

pwc

INTRODUCTION

This paper introduces a new perspective on the impending General Data Protection Regulation (GDPR), arguing that we should not simply view the legislation through a privacy and security lens, but also as a catalyst for improved business operations and innovation. The paper will benefit senior executives interested in understanding the impact of the GDPR on their organisation and the ways in which fundamental changes could be addressed through an effective transformation programme.

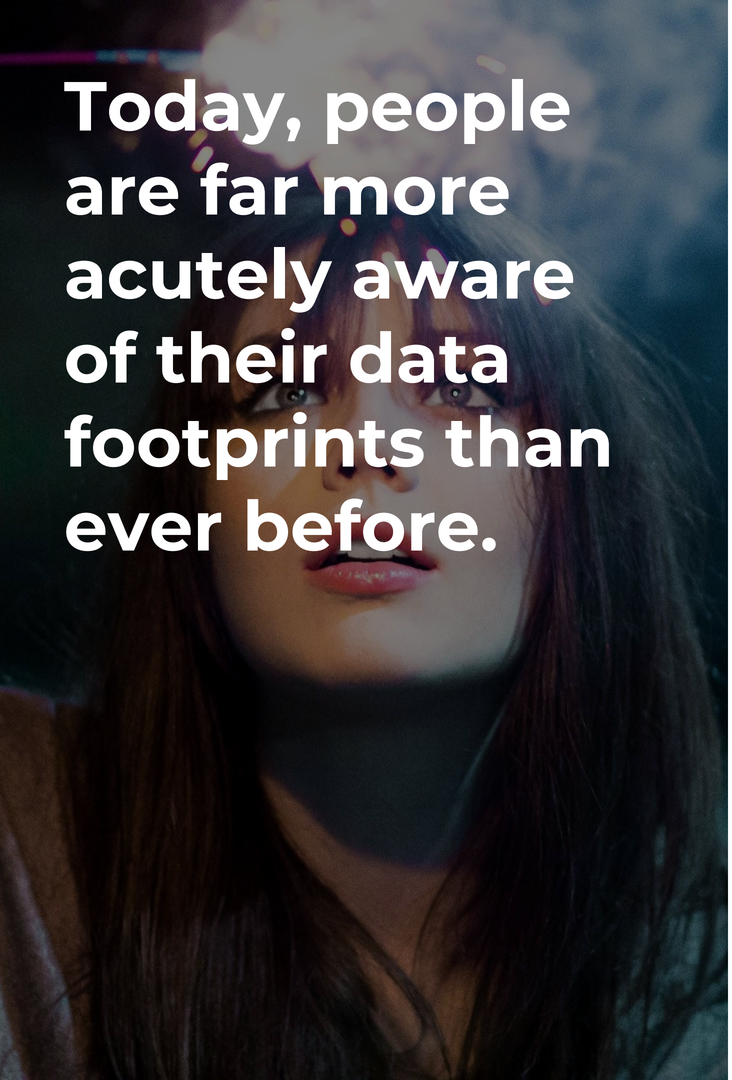
Today's customers are becoming increasingly conscious of their data footprints and, more specifically, the value of the information trail they leave behind. In a recent global survey of over 7,000 customers, Salesforce Research found that 55% of consumers and 75% of business buyers now expect to receive personalised offers from companies with whom they have shared their personal data. No longer satisfied with the immediate benefits provided by service providers or their connected smart devices - laptops, mobile phones, fitness wristbands, smart meters - today's customers demand further exchanges of value from their personal information and activity history, understanding that parting with their data can offer them a superior experience.

These shifting customer perspectives on data and its potential value have already created a raft of opportunities for ambitious organisations, who have been able to deliver more intelligent and unique products, offers and experiences than ever before. However, these organisations have also needed to accept a new and complex responsibility for securing personal information. And it is a responsibility that is set to become an even greater burden in the future.

In May 2018, a new General Data Protection Regulation (GDPR) will impose a radical, much tougher data protection framework on Europe and the wider world for the processing of personal data. Understanding and complying with this legislation will be essential, not only because of the substantial penalties (4% global turnover) and class actions (no damages needed) of failing to do so, but also because of the corresponding risks to, for instance, reputation and operations.

It goes without saying that many businesses will need to (and have started to) revisit their core processes and procedures in order to remain compliant. However, rather than viewing this as a matter that rests solely on the shoulders of privacy and security owners, leading organisations need to view the new GDPR as a catalyst for improved business operations and innovation. In this paper, we show you how this can be achieved through pragmatic and holistic business transformation.

Source(s): “State of the Connected Consumer”, Salesforce Research, 2017



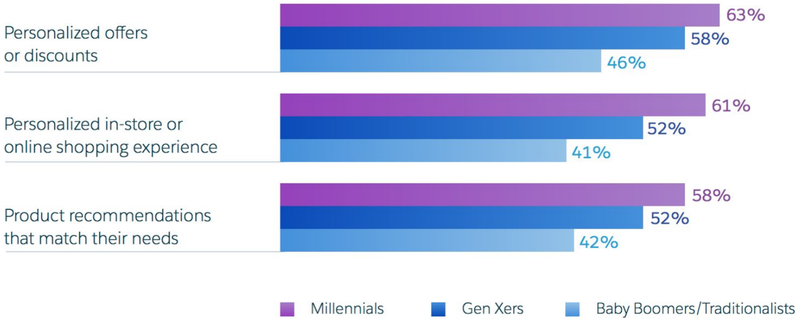
Today, people are far more acutely aware of their data footprints than ever before.

With the booming adoption of connected devices, today's customers are far savvier regarding their data than ever before: they are better informed as to what data they should share with brands, and what to expect in return. Consequently, a trend can be seen in the increasing number of customers willing to share their data for more personalised experiences. And it is looking likely that this trend will continue as millennials' influence on the marketplace increases. Having grown up in the digital age, and willing to attempt virtually anything using their smartphone, this generation has come to expect more intelligent and uniques experiences that cater to their individual needs. Companies that fail to deliver risk aggravating a significant portion of their customers.

Customers Are Willing to Share Data for Personalization

Most customers understand that personalized journeys are created by brands that collect and integrate data. Sixty-three percent of millennial consumers agree they're willing to share data with companies that send personalized offers and discounts.

Percentage of Consumers Who Strongly Agree or Agree They're Willing to Share Personal Data in Exchange for the Following



Source(s): "State of the Connected Consumer", Salesforce Research, 2017

This has created a raft of new opportunities as well as responsibilities for businesses over the past few years.

Many companies have seen this new dynamic as an opportunity to innovate, putting customer expectations at the centre of their organisation and using data shared by customers to form insights that can drive **business** operations, improve customer **experience** and help shape the development of **technology**. At the same time, however, risks have emerged from the processing of personal data, meaning organisations have far greater responsibilities to protect their customers' information. Where companies have failed to do so, they have incurred financial penalties and huge reputational damages.

	BUSINESS	EXPERIENCE	TECHNOLOGY
OPPORTUNITIES	Business **operations driven by insights** from analysis of employee and customer data	Deliver more **intelligent and personalised experiences** than previously possible	Build **technical solutions fuelled by analysis and learning** from internal and external data sources
RESPONSIBILITIES	Business governance, operations and procedures need to provide **adequate data protection**	Experiences need to adequately **inform the customer of use of personal data**	Technology needs to maintain data accuracy, adequacy, and achieve principles based outcomes (e.g. access, portability, suppression, deletion)

The impending General Data Protection Regulation (GDPR) means organisations will have far more responsibilities in the future.

The new General Data Protection Regulation (GDPR) applies to most entities that process EU data subjects' personal information. Effective as of 25 May 2018, the legislation imposes a radical, much tougher data protection regulatory framework on Europe and the wider world for the processing of personal data, with substantial penalties (4% global turnover) and class actions (no damages needed). It stipulates that controllers *and* processors of personal data shall act lawfully, fairly and transparently in their use of personal data and how they deal with the people to whom the data relates. Consequently, businesses will have a number of additional responsibilities that they need to honour if they are to remain compliant.

CHANGES IN RESPONSIBILITIES

BUSINESS

The GDPR will require organisations to **address their existing operational procedures and processes** as follows:

- *Data Processing and Processes must be auditable*
- *Enhanced inspections & audit*
- *Enhanced Governance and Accountability*
- *Formalises Data Protection Officer role & responsibilities*
- *Privacy by Design built in to all new initiatives*

EXPERIENCE

The GDPR could require organisations to **reimagine their existing customer journeys** to comply in the following ways:

- *Greater transparency about how they use personal data*
- *Increased consent and compliance rules*
- *Provide simple access rights… with SLAs*
- *Mandatory breach disclosure (respond and notify within 72 hours)*
- *Right to be forgotten*

TECHNOLOGY

The GDPR will require organisations to **update their existing systems** to comply in the following ways:

- Usage and cyber security controls, limiting what can be done with personal and critical data
- Privacy Impact Assessments and Privacy Audits
- Data minimisation & data portability
- Security response & protecting data (including in an incident)
- Anonymisation/ pseudonymisation to have wider use of data
- Data loss prevention and endpoint security

To succeed in the next data revolution, businesses will need to adopt a vision and strategy with the individual at its core.

The GDPR raises many complex issues for all organisations. Many entities will want to prioritise how they tackle the challenges of the GDPR, which may include taking a risk-based approach so that critical economic and risk issues are addressed first. In our experience, however, optimum programme design begins with a clear vision, which states the objectives, provides an ongoing reference point for the future to ensure that the business priorities are always kept at the forefront, and *places the individual at its core*. Once the vision is agreed, a strategy can be developed, and then the programme structures can be put in place. We expect that regulatory investigations and litigation under the GDPR will hold organisations to account for their vision and their means for achieving it.

The GDPR creates some new rights for individuals and strengthens some existing rights:

The right to be informed	tell individuals what personal data is held relating to them, why, and how it's used
The right of access	know where all Personal Identifiable Information (PII) is held and be able to provide access to this data including historical, in all its forms
The right of rectification	allow individuals to retrieve, review and correct any incorrect personal data
The right to erasure	delete data if requested by the individual and provide evidence of having done so (unless the organisation has a legitimate reason to retain it)
The right to restrict processing	be able to restrict use/processing of data, including by 3rd parties / outsourcers
The right to data portability	be able to retrieve and transfer requested PII data to an individual or to another 3rd party, including to a competitor
Rights in relation to automated decision making and profiling	ensure that no decision making about an individual is done solely on the basis of automated processing of data

What does this look like in practice?

In order to comply with the new General Data Protection Regulation (GDPR), companies should look to adopt a series of best practices across three domains - business, experience and technology (BXT) - in order to reshape their current operations for the next data revolution. Whilst these best practices are legislatively designed to improve the privacy and security of the personal identifiable information of individuals, transforming business operations in the ways suggested can also help organisations deliver in more ethical, sustainable and effective ways than they may have previously.

BUSINESS

Organisations should look to reduce operational complexity, improve governance, optimise partnerships and ensure auditability in order to comply with the GDPR. In doing so, companies can standardise and simplify their existing policies and procedure to dramatically improve business operations.

EXPERIENCE

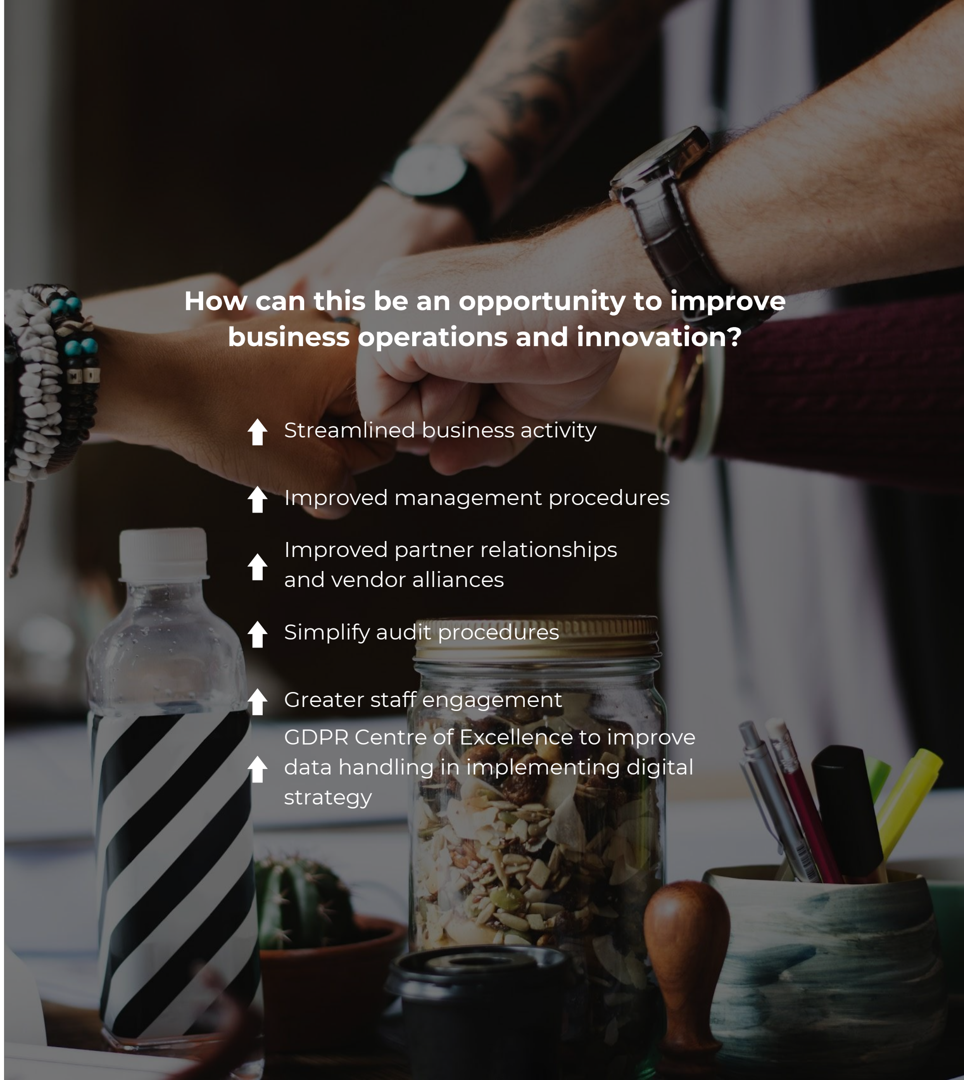
Organisations should aim to create greater transparency, privacy, simpler access to their data and clearer consent points in order to comply with GDPR. In doing so, companies will create more informative and ethical experiences, designed with the customer’s benefits at the core.

TECHNOLOGY

Organisations should look to reduce technological complexity, improve security, optimise incident response times in order to comply with the GDPR. In doing so, companies will have more robust technical architectures and processes in place at the core of their business operations to prevent data loss and protect data in an incident.

Business

- **Leadership:** The protection of sensitive data needs to be driven by leadership and embedded in the business with the appropriate cyber security. This should not only include ensuring that the appropriate strategies are in place to protect data, but also that the culture of the organisation does not expose the business to additional risk and the business needs to be ready to respond to a breach.
- **Reduce complexity:** Whether through a history of mergers and acquisitions or organisational silos, personally identifiable data has the potential to be created and disseminated across an organisation often in completely different ways. Businesses need to reduce complexity to understand what data is held within their organisation, its characteristics and the highest risk areas.
- **Improve governance:** Due to the evolving nature of personally identifiable information and governance of such data, organisations have struggled to put the right ownership and accountabilities in place to control it. Going forwards, organisations need to ensure they know who creates, reuses, updates and deletes data within an organisation as well as in 3rd parties, and ensure they are acting in compliance with GDPR and can evidence compliance through a "Paper Shield" (of appropriate auditable policies and procedures).
- **Optimise partnerships:** Companies must understand their full value chain and the 3rd parties involved in controlling or processing data.
- **Ensure auditability:** Companies need to ensure that they are controlling or processing personally identifiable information in a way that is auditable, so that they can prove to regulators that they are acting in accordance with GDPR. This could mean mapping as-is data processes and reengineering these to standardise and simplify, adding policies, processes, standards and

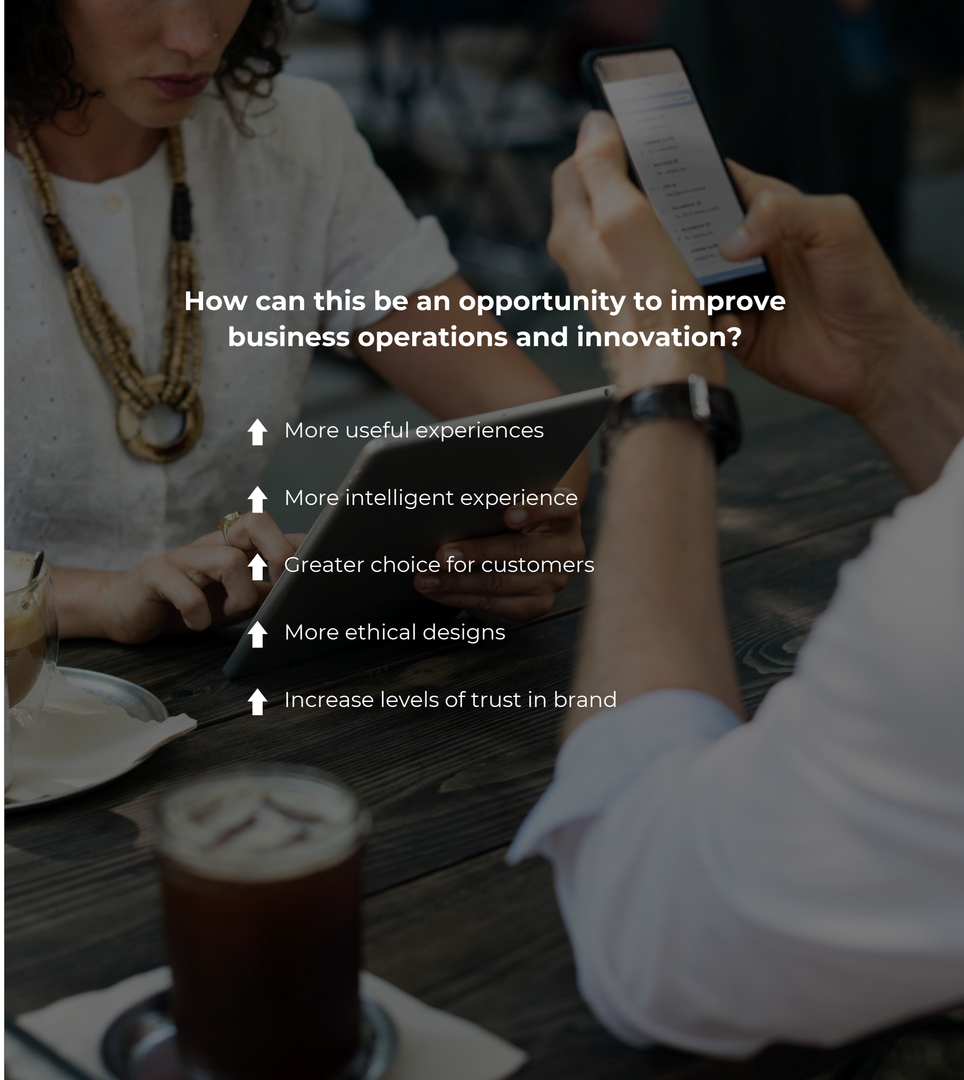


How can this be an opportunity to improve business operations and innovation?

- ↑ Streamlined business activity
- ↑ Improved management procedures
- ↑ Improved partner relationships and vendor alliances
- ↑ Simplify audit procedures
- ↑ Greater staff engagement
- ↑ GDPR Centre of Excellence to improve data handling in implementing digital strategy

Experience

- **Greater transparency:** Companies need to provide greater transparency across the customer journey to ensure that customers are fully informed about how any data they share will be processed by the organisation and third parties.
- **Increased privacy:** Companies need to design customer journeys with privacy at the forefront, allowing individuals to feel secure that their data will only be used for the purposes for which it was collected, and that they have control over how their data is used. This can be achieved by introducing “Privacy by Design” and “Privacy by Default” principles into the customer and employee experience.
- **Simpler access:** Companies need to design, develop and establish a customer experience and an internal capability that can handle the Subject Access Requests (including SLAs).
- **Clearer consent:** The customer experience needs to offer clear points of consent at which customers can agree for their personally identifiable information to be collected and used by an organisation.



How can this be an opportunity to improve business operations and innovation?

⬆ More useful experiences

⬆ More intelligent experience

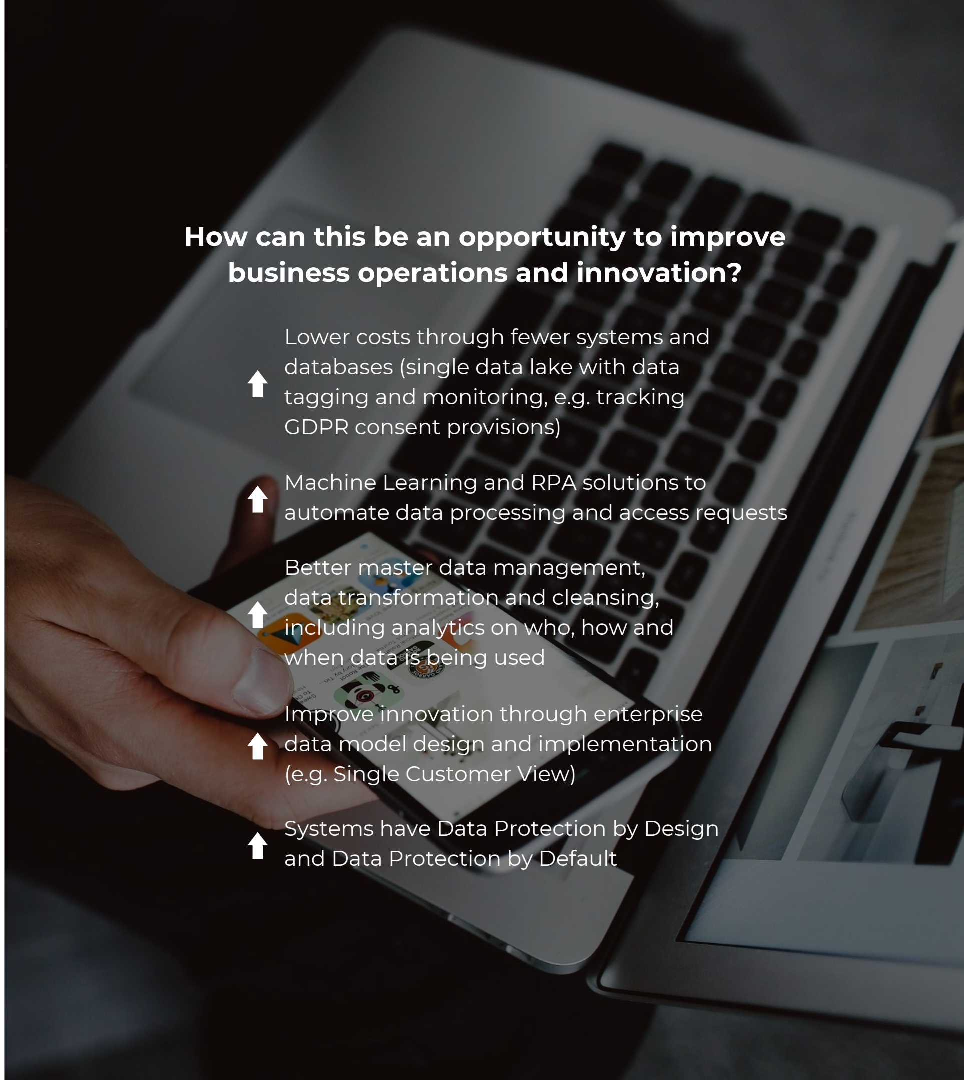
⬆ Greater choice for customers

⬆ More ethical designs

⬆ Increase levels of trust in brand

Technology

- **Reduce complexity:** Allied to the business complexity, IT systems (historical and current) create complexity in identifying and controlling the legacy data. Companies need to simplify system usage so they understand where data is being held and can retrieve, access, manage, delete and port it when needed (e.g. citizens exercising their legal rights to access and transfer their data).
- **Improve security:** Companies need to insure that the systems they put in place meet the security standards suggested in the GDPR. This includes: pseudonymisation, encryption of personal data and the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services (e.g. Data loss prevention and endpoint security, and protecting data in an incident).
- **Adequate response times:** Companies need breach detection and response technologies that have the ability to restore the availability and access to personal data in a timely manner (72 hours) in the event of a physical or technical incident.
- **Increase agility:** Companies need to deploy systems flexible enough to ensure that they can move with agility should they need to rapidly respond to customer data requests or security breaches. This could include harnessing accelerators (e.g. robotic process automation [RPA]).



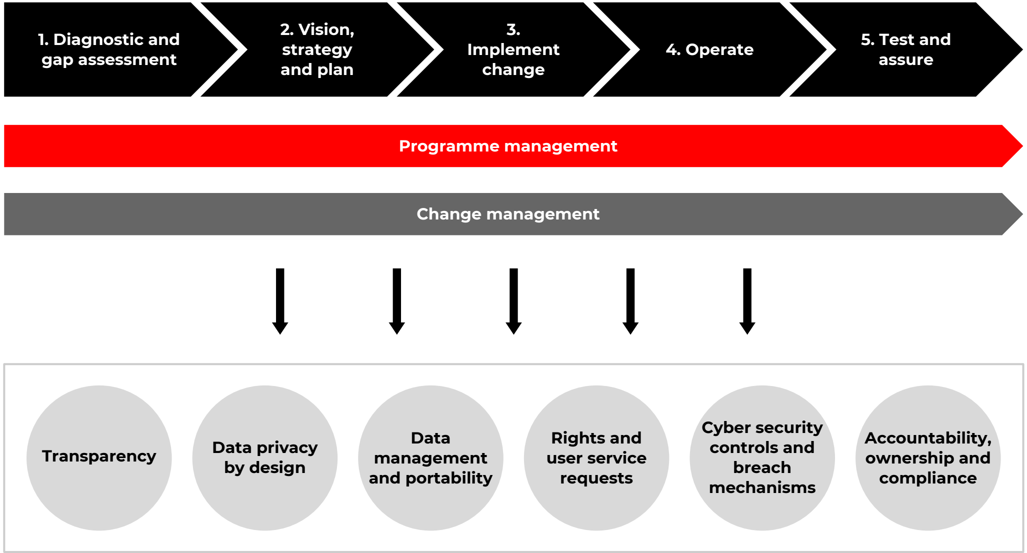
How can this be an opportunity to improve business operations and innovation?

- ⬆ Lower costs through fewer systems and databases (single data lake with data tagging and monitoring, e.g. tracking GDPR consent provisions)
- ⬆ Machine Learning and RPA solutions to automate data processing and access requests
- ⬆ Better master data management, data transformation and cleansing, including analytics on who, how and when data is being used
- ⬆ Improve innovation through enterprise data model design and implementation (e.g. Single Customer View)
- ⬆ Systems have Data Protection by Design and Data Protection by Default

How can companies transform to meet the new GDPR and improve their business operations?

Once a business has established their vision for operations after GDPR, they should begin a systematic programme of change. Regardless of whether an organisation is at the start of their journey or midway through programme delivery and looking to make informed risk-prioritised adjustments to their business or deliver holistic transformation across operations, customer experience and technical solutions, they can follow the same approach to deliver the required outcomes.

Transformation plan and objectives:



1. Diagnostic and gap assessment

2. Vision, strategy and plan

3. Implement change

4. Operate

5. Test and assure

Programme management

Change management

Transparency

Data privacy by design

Data management and portability

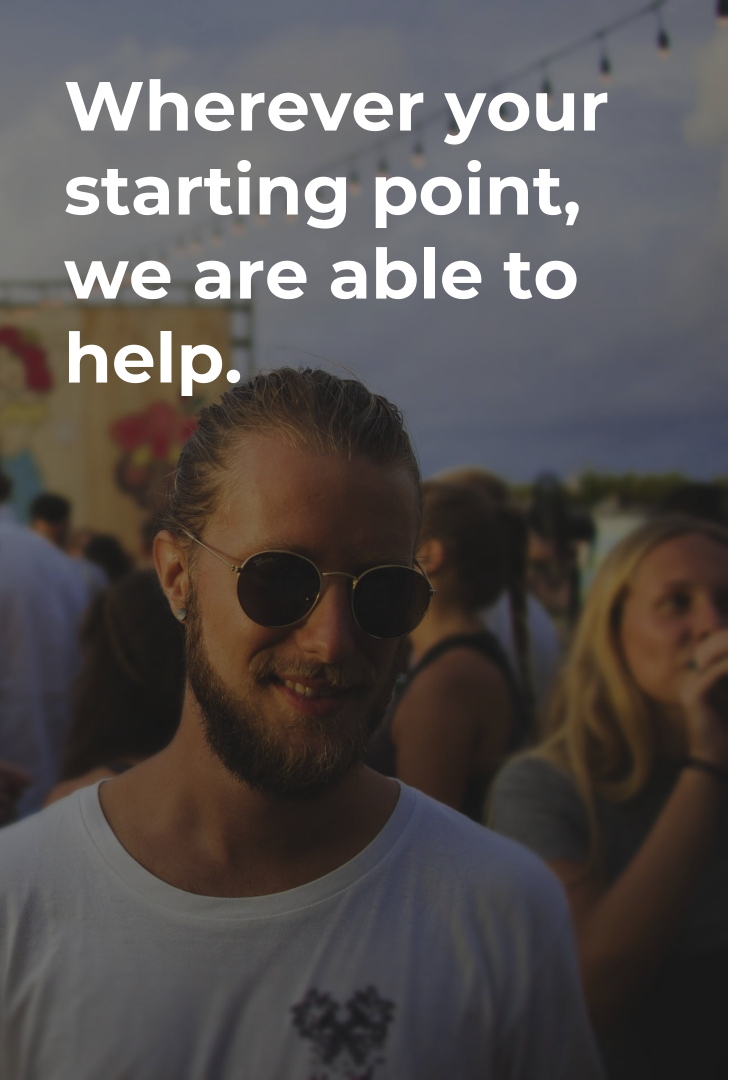
Rights and user service requests

Cyber security controls and breach mechanisms

Accountability, ownership and compliance

	1. Diagnostic and gap assessment	2. Vision, strategy and plan	3. Implement change	4. Operate	5. Test and assure
PWC	**Use Readiness Assessment Tool (RAT) and Technology Assessment Tool (TAT) to diagnose current state of organisation and cyber security.**	**Run programme of workshops to establish vision, strategy and plan for change, and deliver blueprint.**	**Run change management programme and support technical implementation to embed GDPR culture and behaviours.**	**Support governance and operation of new business model.**	**Deliver assurance review of new business operations and monitor GDPR compliance.**
BUSINESS	Assess current compliance to GDPR regulations based on existing operations and procedures.	Identify data protection objectives and priorities for the business, including new operations framework, sponsorship and value case and incident response planning.	Create a record of all data processing activities and establish robust processes for incident response, breach resolution and data subjects requests.	Operate at required level of data protection & information governance standards.	Review effectiveness of governance, operations and compliance of contracts to GDPR. Conduct crisis exercises to test the ability to respond to a breach.
EXPERIENCE	Assess current customer and employee journeys to understand existing data collection points and any special characteristics.	Define basis for data processing for customers and employees across engagement journey.	Build the evidence “Paper Shield” including privacy notices, policies, contracts and terms. Obtain appropriate consent for customer and employee data.	Deliver updated customer and employee experiences and compliant data retention strategy.	Monitor and maintain customer and employee experiences and compliant data retention strategy.
TECHNOLOGY	Assess what data is stored, where it is and where greater protection of data is required and close any key cyber security gaps.	To be migrated To be transformed 🟥 To be rebuilt Update data registry, data management strategy and systems architecture, including GDPR-compliant vendor selection.	Migrate Transform Rebuild Update technology and implement single ‘personal information data’ source (removing legacy) and update cyber security to protect key data.	Optimise data use, including further consolidation and continue to retire legacy infrastructure.	Conduct regular assurance activities to ensure cyber security around the protection of data remains appropriate considering new threats and update technology to meet new regulations.

Wherever your starting point, we are able to help.



Whether you are looking to focus on risks and managing the essentials, or want to pursue a full business transformation, we have the end-to-end skills and capabilities to able to provide support:

1. Initial assessment and roadmap: Our initial assessments (Readiness Assessment Tool [RAT], Technology Assessment Tool [TAT], Special Characteristics Workshop [SCW], cyber security assessment) can be a useful place to start. These 'Intelligent Questionnaires' are designed to ask closed questions about clients' business and technological readiness for the GDPR, based around PwC's maturity matrix. The questions are linked to the requirements of the GDPR and deliver 'intelligent' data that provides organisations with a high level view of data protection compliance across your business functions and local offices, including: cyber security, threat intelligence and incident response. This gap analysis can be used to form a roadmap.

2. Business change and technology support: For clients midway through their GDPR adjustment programme, we can help by offering delivery accelerators, business change support and technology alliances with GDPR-compliant vendors. Our specialists will work with your teams to drive improved programme performance and make sure that the right changes are made within your organisation, technology and enterprise data model, and that they are communicated in the most effective ways with your workforce.

3. Review and evaluation: For clients who are further into their change programmes and looking for assurance that they meet the GDPR, we can offer an assurance review. We look at the adjustments you have made to your organisation and ascertain whether these will meet new standards of compliance.

PwC Capabilities			
Legal & Privacy	**Consulting**	**Assurance & Cyber**	**Data & Forensics**
Legal support and Interpretation of opinion; GDPR strategy; deep privacy expertise; privacy by design; privacy impact assessments; personal data breach notification; "Data Subject Rights handling"	*Digital & business strategy; process development and change management; technology implementations; training & awareness and fit with digital strategy.*	*Programme assurance; controls advice and reviews; internal audit; information governance; cyber security & incident response expertise.*	*Data expertise, including: Search and e-discovery; data mapping; data classification; weeding and de-duplication; digital investigations.*

If you are interested in learning more, please contact any of our GDPR specialists, or a sector representative.

GDPR Practice Leader Legal & Privacy

Stewart Room
PARTNER
stewart.room@pwc.com

Consulting Lead

Mike Greig
PARTNER
mike.greig@pwc.com

Cyber Security Lead

Zubin Randeria
PARTNER
zubin.randeria@pwc.com

Risk Assurance Lead

Andrew Paynter
PARTNER
andrew.paynter@pwc.com

Data & Forensics Lead

Umang Paw
PARTNER
umang.paw@pwc.com

Private Sector

Michael Orr
PARTNER
michael.g.orr@pwc.com

Financial services

Jonathan Turner
PARTNER
jonathan.v.turner@pwc.com

G&HI

David Quinn
PARTNER
david.quinn@pwc.com

Technology & Data Lead

Sultan Mahmood
PARTNER
sultan.mahmood@pwc.com

Cyber Security Programme Lead

James Rashleigh
DIRECTOR
james.m.rashleigh@pwc.com

Technology & Data Programme Lead

Pat Beattie
DIRECTOR
patrick.beattie@pwc.com

Technology & Data Programme Lead

Peter Almond
DIRECTOR
peter.almond@pwc.com

GDPR Process & Programme Lead

Jenny Etherton
DIRECTOR
jenny.etherton@pwc.com

GDPR Process & Programme Lead

John Dunlop
DIRECTOR
john.dunlop@pwc.com

GDPR Process & Programme Lead

Mita Dave
DIRECTOR
mita.dave@pwc.com