IBM

The Journey to Value

Creating a sustainable, governed data asset for GDPR and beyond

IBM

1. GDPR as a business opportunity

With the introduction of the General Data Protection Regulation (GDPR) and its enforcement from 25th May 2018, a new balance will be created between commercial interests and consumer rights around personal and sensitive data. All individuals possess personal data which needs to be shared with organisations – customers during transactions, employees at work, business partners under contract. Engaging positively and responsibly with these data subjects is the intended outcome of the Regulation and will ensure business is sustainable as well as capable of continued innovation.

In the run-up to this new environment, much will be done to educate individuals about their new rights and the need for businesses to process their data. At the moment, awareness is low – just 10 per cent of consumers surveyed said they are fully aware of GDPR (Source: "GDPR Impact 2017", DataIQ commissioned survey of 1,001 UK consumers conducted by Research Now, February 2017). But just as data security has become a mainstream issue, so will data protection. The difference is in the opportunity for demonstrating the upside of data sharing, rather than defending against the downsides of data breaches.

A new approach to the data-value exchange is being built by leading data-driven organisations, which helps to enable access and control by data subjects while supporting core business processes with sustainable, governed data flows. GDPR requires a review of end-to-end data processing – the outcome should enable both data subjects and the business.

Adopting this positive approach can help to create value for the business in two dimensions:

Brand value – as individuals become aware of their new rights, they will gravitate towards brands which deliver the best enablement and experience. Leaders may win trust and commercial advantage as a consequence.

Business value – by streamlining data policies, introducing more efficient and integrated data processing, and ensuring operational systems are aligned with what GDPR requires, the business can achieve cost-savings.

2. GDPR – building on strong foundations

By the time GDPR starts to be enforced, it will be 20 years since the existing Data Protection Directive was introduced. In that time, everything has changed – the types of data being created, the processes used to capture and govern it, the systems used to manage, analyse and deploy it. Organisations which already respect the core principles within the law should be well placed to adapt to the Regulation. The expansions and enhancements which it introduces will need careful handling, however.

Data is more personal –

GDPR expands the definition of personal data to cover almost anything that can identify an individual, such as where they are (location), what content or apps they are consuming (behavioural), what device they are using (device ID). Unstructured data, such as customer comments, reviews, blog posts, customer service notes, account management emails, even internal messaging, also needs to be governed.

More access and consent –

in addition to existing rights, such as access and rectification, individuals gain enhanced rights, including the ability to withdraw consent, to move personal data to another provider and even to request data is deleted.

European, everywhere –

any data subject in the European Union can expect these rights to be protected regardless of where their data is held or processed. When data is transferred outside the EU, these rights follow, so moving personal data between territories will need to be done with care.

End-to-end responsibility –

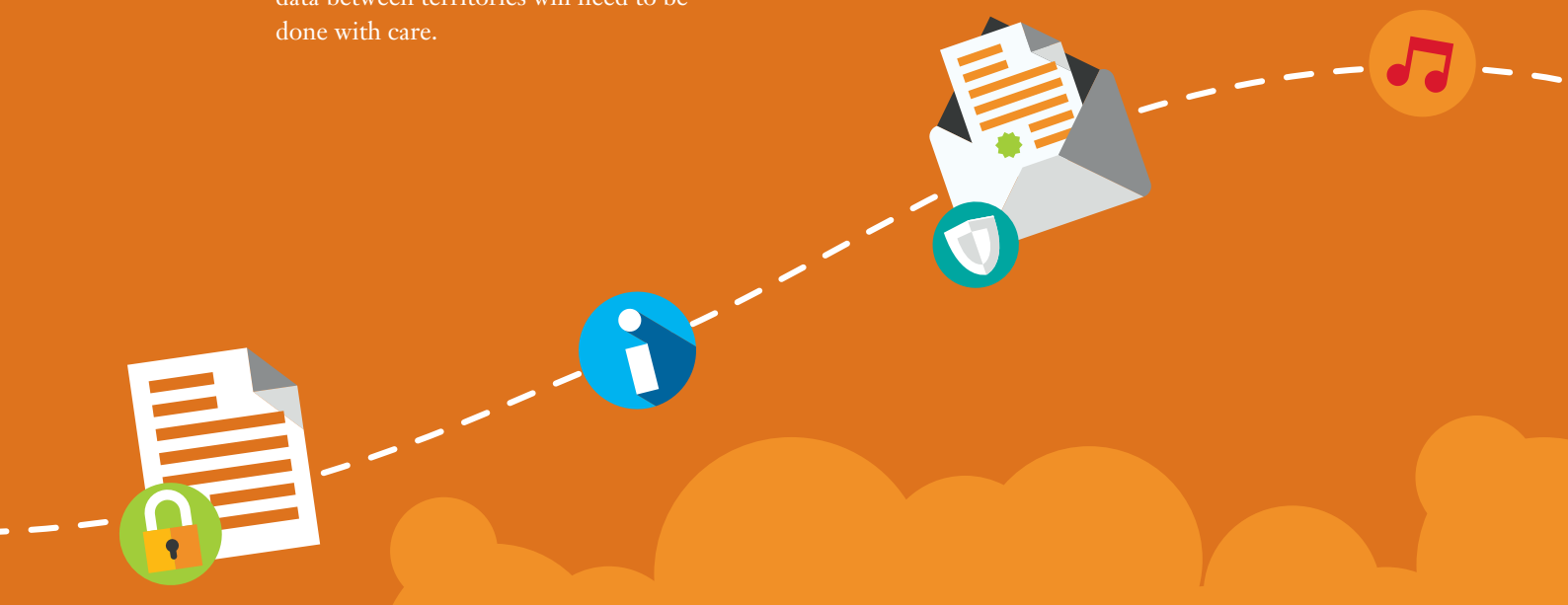
as well as respecting GDPR as an organisation, data controllers have to validate that their business partners (data processors) are also working to the Regulation. Both parties carry obligations to ensure data security and there are new duties around reporting data breaches.

New data duties –

a range of new requirements is introduced, most notably the obligation to have a Data Protection Officer, but also the adoption of new data governance strategies and a risk-based approach.

Stronger enforcement –

enhanced powers for Data Protection Authorities are central to ensuring GDPR is enforced, most notably the potential ability to impose a fine of up to 4 per cent of annual global group turnover or €20 million, whichever is the greater.



3. Key steps on the journey to value

The intention of GDPR is to provide a greater balance between legitimate business interests and the rights of the individual data subject. Addressing this through a creative, transparent and enabling approach is the key to meeting the new demands of the Regulation and to finding new value from a sustainable, governed data asset.

IBM has identified five key steps for organisations to consider:

Governance – central to GDPR is cross-functional involvement in the way personal data is captured, processed, managed, secured and deployed. This starts at a strategic level through the adoption of Privacy by Design in the development of new data-dependent processes, combined with Privacy Impact Assessments to identify risks and exposure of any sensitive data elements.

Explaining to individuals in a clear, transparent way why their data is needed, how it will be used and managed and for how long will require privacy notices to be reviewed. The specific consents and wordings should be recorded against each record. Governing across the organisation becomes the responsibility of a Data Protection Officer (DPO) who is required to have specific responsibilities, status and support. Existing roles may be suitable for migration into this position, with additional training, or a new hire may be required. Alternatively, a shared, outsourced DPO can be used as a lower-cost alternative.

Third parties, such as downstream data processors, may be brought under the umbrella of this governance. It is important to validate that these business partners are following GDPR and this should be detailed in all contractual arrangements.

Rights and processes – with data subjects given enhanced rights, such as consent withdrawal, portability and deletion, alongside their existing rights, such as rectification and Subject Access Requests, significant development may be required to ensure these are delivered. Technical solutions will have a key role to play, alongside revised strategies.

Business processes may also need to adapt in order to be GDPR-ready. Frontline functions such as customer relationship management which are heavily dependent on personal data will need to be reviewed and re-engineered as necessary. Back office functions, such as HR, also need to be brought in line to support employee rights and avoid risks from ungoverned personal data.

Data – data flows across organisations from every business process and channel as well as from the outside, via digital marketing, distribution partners and other market contact points. If your business model is fundamentally based around this flow of personal information, then a data discovery and audit programme is essential. Mapping which data types are in use, where they are held and whether they are sensitive will describe the landscape through which the organisation has to journey in order to meet GDPR.

Integration of all of these data sets to create a 360-degree view will become a key enabler – creating a single customer view ensures that individuals can access, control, correct or extract their personal data as required by the Regulation, while forming the foundation for future data-driven value creation. It also helps to ensure that appropriate information lifecycle management can be applied, including, if requested and legitimate, deletion of a customer's record.

Data security – keeping personal information secure is central to the data protection mandate. As well as protecting a valuable business asset, data security should also form part of the promise made to customers, who are increasingly concerned about their personal risk from data breaches and losses. Investing in proper data security can be a competitive differentiator in the post-GDPR era of trust-driven relationships.

It is likely that one of the most challenging demands of GDPR will be to notify the regulator of any data breach within 72 hours of becoming aware of it, and to tell the individuals affected within a reasonable period of time. Through the adoption of industry-standard data access management and security monitoring tools, plus improved orchestration of incident response capability, an organisation can prepare itself for this stringent obligation.

People and communications – the human dimension of becoming GDPR-ready requires a combination of formal communications and constant reinforcement. Role-specific messages as well as umbrella enterprise-level communications should spell out new working practices and what the new organisational culture should look like.

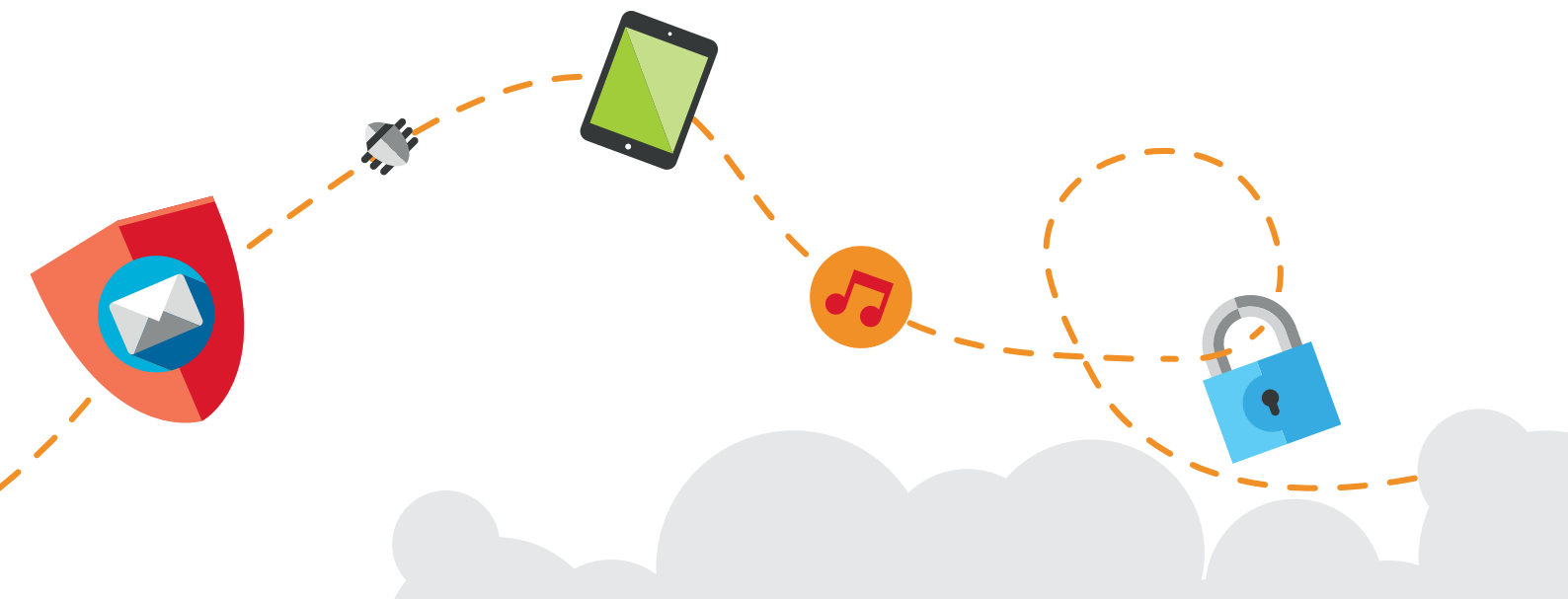
Building a workforce that is clear about the need to treat personal information as a vital business asset and to respect the rights of individuals around their data may require significant upfront training and ongoing reinforcement. Well-structured training programmes, especially those delivered as a service, should to be built into the GDPR programme.

4. IBM as your guide on the journey

IBM can assist you with your GDPR readiness programme through a full end-to-end solution. With our skills in global business services, our proprietary technologies and our innovations around privacy management, we can help your business to get ready.

Plus, we are on this journey too. IBM is undertaking its own GDPR project, so we can share the insights and learnings from our direct experience, as well as the success factors we have learned from supporting our clients.

- **Experienced consultants –** domain experts with deep knowledge of data protection**.**
- **Business change management –** intellectual capital, resources and tools to help transformations of business processes.
- **Technology solutions –** from data management and information lifecycle management through to information security and incident reporting.
- **Holistic offering –** a clear focus on critical changes needed by 25th May 2018 as well as long-term value generation.



For more information

To learn more about the GDPR and IBM solutions to help you protect, govern and know your data, contact your IBM representative or visit:

ibm.com/gdpr

IBM United Kingdom
PO Box 41
North Harbour
Portsmouth
Hampshire
PO6 3AU

Produced in the United Kingdom
March 2017