White Paper

Defining the data powered future

An Experian guide to EU GDPR

Foreword:

Setting new standards for the digital age

A core theme of the European Union's General Data Protection Regulation (EU GDPR), which is to keep consumer interests front of mind at all times, mirrors sound fundamental advice for all companies. Customer-centric business practices are especially essential in the data-driven age, driving innovation and opportunity.

The transparent, secure and effective use of data has transformative potential for consumers and businesses. But consumers must feel comfortable and in control of its opportunities, and there is a clear role for our industry to play in addressing their understandable concerns around privacy and security.

In particular, there is a need for more openness about how data is collected and used for the benefit of consumers. In business, we are all aware of the advantages that data-driven technology can bring. Yet the way data is harnessed for good hasn't, to date, been a central part of the prevailing 'data narrative'.

At Experian, we believe that organisations have a responsibility to build that trust with consumers by demonstrating their integrity through better data stewardship, transparency and accuracy. And building that trust, in turn, will deliver better business outcomes.

It is interesting to note the evidence that in some circumstances value and convenience are superseding privacy and security concerns. Consumers are prepared to share data with organisations they trust if they feel there is a fair exchange going on.

This behaviour only increases the onus on businesses to earn that trust. Nothing less than the highest standards can be applied when it comes to managing people's data. Lack of transparency, poor practice, and unclear messages will do more than damage a reputation – they will jeopardise the consumer's willingness to share their data in future.

At Experian, we process over 1,151 billion records a year, with a global segmentation of more than 2.3 billion consumers in more than 30 countries, and demographic data on over 700 million individuals and 270 million households combined. It's a responsibility we take very seriously.

We have always aspired to set new benchmarks for best practice in our operating standards and our approach to data stewardship. As a trusted data custodian for millions of consumers, we aim to unlock the power of data to create opportunities for individuals, businesses and society.

The world is becoming more connected every day, and if businesses are serious about keeping up with the change, a truly holistic approach to managing all this data is required. One which protects our customers and our products from risks, such as an ever-increasing array of cyber threats, while ensuring the customer journey is as relevant and fluid as it needs to be.

With the advent of GDPR, this type of joined-up thinking will need to become the new normal, as the "datafication" of our world continues. I would encourage businesses of all shapes and sizes to take the opportunity that this moment brings. Now is the time to create a truly consumer-centric approach to data governance and strategy, and to secure your customer's place at the heart of your data powered future.

At Experian, we look after a global segmentation of more than 2.3 billion consumers in more than 30 countries - a responsibility we take very seriously.

Charles Butterworth, Managing Director, UKI & EMEA, Experian

Introduction:

A brief history of EU GDPR

Driven by the proliferation of connected technology, organisations of all shapes and sizes are now in possession of more customer information than ever before. The current legislation was drawn-up at a time before smart-phones, search engines and social media even existed. The EU's General Data Protection Regulation (GDPR) is the result of four years of work by the EU to bring data protection legislation into line with the myriad ways that data is now intertwined in our daily lives.

With this explosion of data comes greater responsibility. As the data stack grew, inexorably, regulators recognised that existing laws were insufficient to manage how data is being governed. Regulation needed to find a way to keep pace with the rapidly evolving digital landscape.

In response, the EU drafted a new set of comprehensive regulations, the GDPR, which becomes directly applicable in member states from 25th May 2018, two years after it came into force.

For businesses not just in Europe but across the world, this is a significant moment. Despite the ambiguities of Brexit, the UK government has made clear the UK will adopt GDPR even after it leaves the EU.

In fact, the GDPR is being looked upon as a global model for future data protection regulation.

Despite the publicity surrounding GDPR, and its significance for businesses, awareness has not yet translated into a high level of readiness. A recent Experian survey[1] found that only 7% of businesses are 'very prepared', 48% say they are 'somewhat ready', and over 25% are 'not very' or 'not at all' prepared for the new rules. With less than a year left until GDPR comes into force, it's clear that many organisations risk being left behind.

4.1%

Only a small minority (4.1%) of respondents have no awareness of GDPR

7%

7% are 'very prepared'

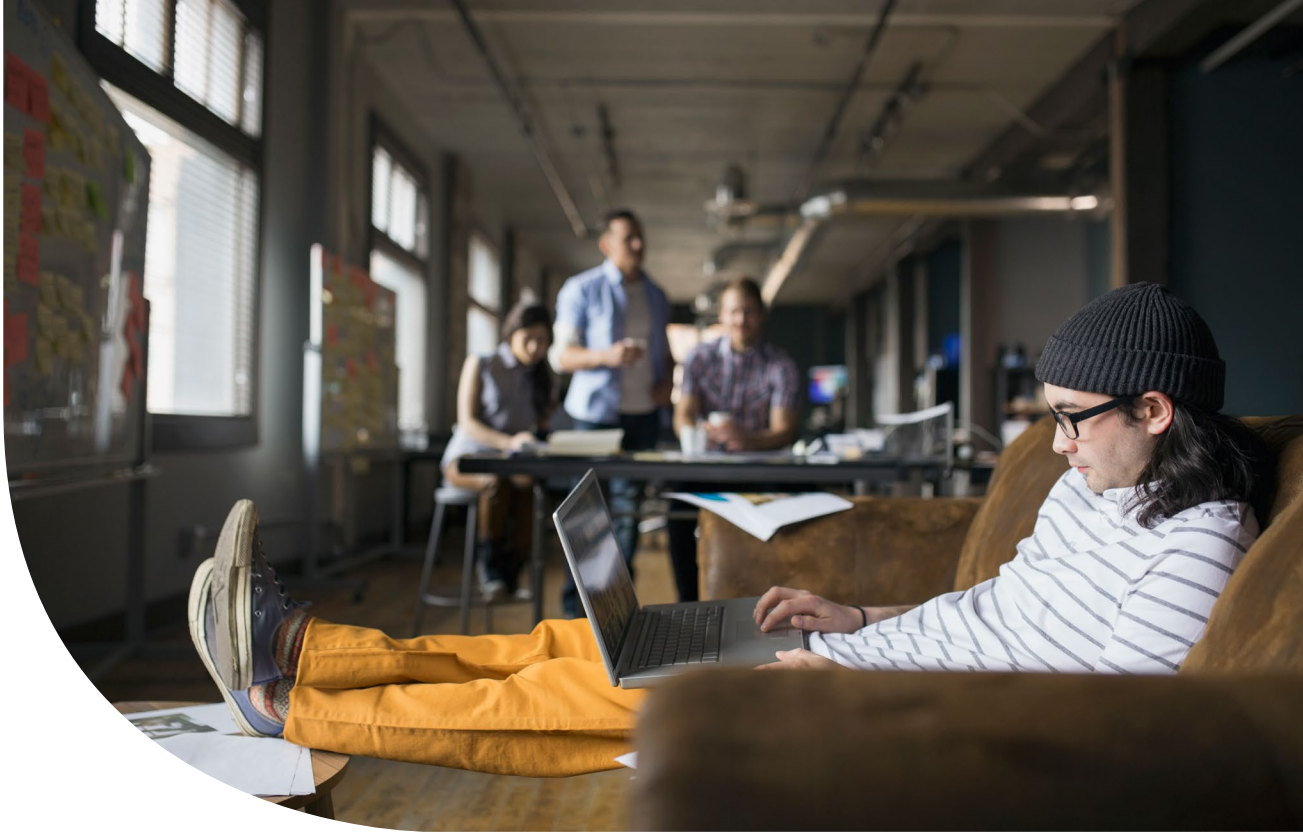
48%

48% say they are 'somewhat ready'

25%

Over 25% are 'not very' or 'not at all' prepared for GDPR

[1] Experian / Data IQ , General Data Protection Regulation - Identifying its impact on marketers and the consumer's moment of truth, 2016



How is personal data regulation changing?

Currently, in the UK, businesses operate under the Data Protection Act 1998 (which implemented the EU Data Protection Directive 95/46/EC), while other countries across Europe have their own local law incorporating the EU's Directive.

In the twenty years since the Directive was introduced, the world has become digital. As a result, we have seen a radical shift in the volume, variety and the speed of data that is produced. Discussions have been ongoing in the EU for many years about the implementation of a new data protection regime to address these changes in how our data is used. It's been a race between changing technologies leading to the unlocking of more data, and regulators' ability to keep pace with these technologies and understand the wider changing environment.

The European Parliament and the Council formally adopted the GDPR in April 2016. We are now in the implementation period, where businesses need to comply with its provisions in full by 25th May, 2018.

The GDPR focuses heavily on protecting individuals and their data. This has also been intentionally agreed as a regulation (as opposed to another directive) which means it will be a single piece of legislation directly applicable across all EU member states. It includes a number of new and increased obligations businesses will need to adhere to.

Much attention has been placed on the fines for non-compliance, but there are worthy 'carrots' to balance the stick of regulatory obligation. Chief amongst these is the opportunity for organisations to earn the respect of their customers by adhering to the new regulation - improving customer trust is what GDPR has been designed to support.

When data is put under increased scrutiny, then, by definition, it is taken more seriously. Its role in how a company functions will become clearer, and companies will need to be quick to examine the value of their data and the benefits of keeping that data fit for purpose and well protected.

7 ways that meeting the requirements of the GDPR can help to boost your business:

1. Clearer view of customer base and relationships
2. Ability to more accurately target new customers
3. Enhanced customer experience
4. More accurate lending decisions
5. Improved efficiency
6. Better communication with your customers
7. Added accountability, credibility and trust through transparency

6 key elements of GDPR

1. Rights of Individuals
There has been a desire to strengthen data subject rights within the GDPR. To this end, there are a number of new (e.g. the Right to Erasure or Right to be Forgotten) or enhanced (e.g. Right to be Informed) data subject rights. Two of these, the Right to be Forgotten, and Right to be Informed are explained in a more detail below.

2. Right to be Informed
Businesses need to make sure individuals understand who the controller is that is collecting their personal data and the purposes for which they are processing it. Organisations' privacy policies will need to be updated in line with the requirements of the GDPR. The new principle of accountability in the GDPR means there will be much more of an onus on controller businesses to demonstrate compliance with the data protection principles within the GDPR.

3. Right to Erasure ("Right to be Forgotten")
A Right to Erasure has now been set out clearly in the GDPR which will allow individuals a qualified right to request that their data be erased, provided certain grounds apply (for example, the data is no longer necessary in relation to the purposes for which it was collected). Where relevant, businesses will have an obligation to erase the relevant personal data it holds concerning that individual within a maximum of one month of the receipt of the request.

4. Data Protection Officer (DPO)
Businesses will be required to appoint a DPO to help them comply with all of their obligations under GDPR. This is a designated role with tasks set out in the GDPR, including responsibility for monitoring compliance with the GDPR. It's needed whether the organisation is acting as a processor or a controller where processing operations require regular or systematic monitoring of people on a large scale.

5. Obligations on data processors

Under the Data Protection Act 1998 the statutory obligations are on data controllers only. However, under the GDPR, data processors will also have obligations, for example, the processor will have a responsibility for implementing appropriate technical and organisational measures for the security of personal data during its processing activities. Processors will be legally accountable for compliance beyond any contract terms, but reputable data processors will already have many measures in place to demonstrate compliance.

6. Data Protection Impact Assessment

Businesses will need to carry out a data protection impact assessment where the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. GDPR includes a requirement for controllers to report a personal data breach to its data protection supervisory authority (the Information Commissioners Office ('ICO') in the UK) without undue delay and, where feasible, within 72 hours, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Where the breach is likely to result in high risk to those rights and freedoms, the data controller will also need to communicate the breach to impacted individuals without excessive delay.

The value exchange

Today's consumers are far more aware of the value of their data. They are beginning to recognise that they own their data and starting to accept the responsibilities that come with this ownership. That said, this increased awareness has not meant that more consumers are shying away from sharing their data, nor has it therefore hampered the growth of the data market.

In fact, people seem to be increasingly comfortable with sharing their data, on their own terms. A recent Experian survey[(2)] found that 49% of consumers are prepared to give their data to brands they trust, while 69% were happy for brands to use their personal information to send them discounts on products and services that they really want.

[2] Experian/Consumer Intelligence 'Data Preferences' Survey, 2016

Getting ready for the regulation:

The "i's" have it

It is imperative that businesses start to think about their implementation requirements now, so as not to risk falling behind. It's all about building relationships and trust – remembering the people behind the devices and doing your utmost to treat them as you would wish to be treated yourself.

It's likely that businesses will be required to do some real 'soul-searching' as they work through this phase. It's not good enough to feel 'fairly confident' that the data you hold is being used in the interests of the customer. It's a requirement that new levels of scrutiny are applied here, and the customer's perspective is the be-all and end-all guide to whether you are getting it right.

With that in mind, we've created this three step process for organisations to work through in order to help them navigate through and potentially thrive in the new regulatory environment.

"70% companies agree that increasing regulation has driven the need for better data analytics and management"[3]

Soul-searching:

Key questions you need to be asking

- Are we using information in a way that people would reasonably expect? This may involve undertaking research to understand people's expectations about how their data will be used.
- Will our approach to using data have unjustified adverse effects on our customers? Think about the impact of your processing.
- Do people know how their information will be used? This means providing transparency, issuing privacy notices or making them available using the most appropriate channels

[3] Experian Global Data Management Research Report, 2017

"64% of businesses think inaccurate data is undermining their ability to provide an excellent customer experience"[4]

1. "Investigate"

When preparing for GDPR, organisations must make sure that the personal data they hold is accurate and that the collection, storage, use and erasure of that data follow a 'Privacy by Design' approach to systems engineering, which takes privacy into account from inception and throughout the whole process.

Data quality is the first stage in the process. Only after a thorough investigation can businesses understand where they may be exposed and where they need to improve their data management practices.

It's also a good idea to develop a full understanding about what constitutes 'personal data', given the broader GDPR definition. We recommend the allocation of a 'data typology' to all assets, allowing businesses to question which assets could be classified as 'personal' and which might fall into another category.

"Seven in 10 (72%) of companies said that data quality issues had affected trust and perception by their customers"[5]

- Consider the quality and integrity of the personal data you hold. Is it accurate and up to date?
- In terms of retention, do you really need to keep it at all? Ask yourself 'what is the value of this data to the business?' and 'what have we told consumers about how long we will retain their data for?'
- Ask yourself what are main data risks in the business? Create awareness across your structure and set up a privacy task force to inform decision makers on GDPR impact.
- Understand the legal grounds on which you currently collect and use personal data. How are consent, legitimate interests and other grounds used as basis for processing personal data – and record this
- Map the personal data you hold and how this data flows through your organisation (system by system). Identify personal data flows which happen across borders, both to and from other EU member states, and beyond.
- Identify personal data capture points (e.g. online forms, registrations, call centres). Are you validating at point of entry? What are people told about how their data will be used? Check your policies, statements, and notices.
- Categorise your data and associate risk to prioritise activity. Conduct Data Protection Impact Assessments (DPIA) for riskier activities
- Review and update privacy policies and notices: make sure they meet the transparency challenge.
- Review all your third party relationships – processors now have responsibilities.

[4] Experian Global Data Management Report, 2017

[5] Ibid

2. "Improve"

It is a given that with the enhancement in standards of customer data management set by the new regulatory framework, businesses must improve their approach in line with those new requirements.

Organisations need to ensure they are always meeting the rights of the data subject, holding accurate data and improving practices such as data portability and subject access requests, guaranteeing that the consumer's right to rectify, object and have their data deleted is straightforward to arrange.

The increasing number of channels used to collect data can potentially make this transformation complex. Businesses need to control where information is stored, moved and shared. The ability to have a single view on each of your customers will therefore become increasingly important under GDPR.

Some practices you should consider introducing to help with the new requirements set by the GDPR should include the following:

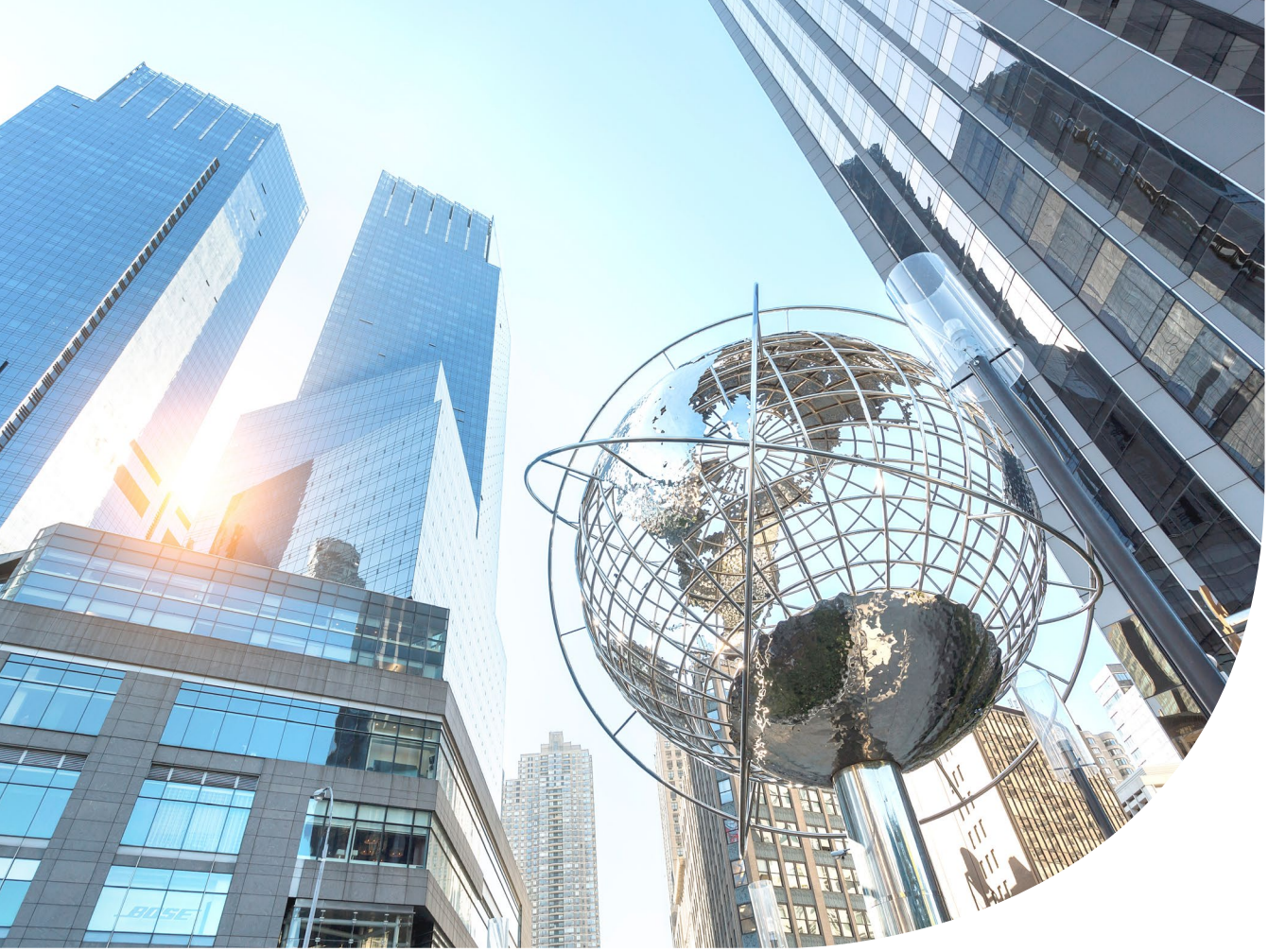
"37% plan to recruit 'data champions' and 'data steward' roles in 2017"[7]

"31% plan to hire a Data Protection Officer in the next 12 months"[6]

- Developing a full 360 view of their customer base, utilising the latest technology, to ensure they are able to keep up to date with customer data across channels. For example, applying a unique customer identifier, commonly known as a customer PIN, helps businesses draw all the information together, even when the data itself is spread across multiple points and is constantly evolving.
- The adoption of compliance 'building blocks' that reflect the key themes of GDPR and demonstrate to the regulator that the organisation is taking active measures to ensure responsibility for effective data protection, including documentation and regular audit processes.
- Introducing a new information governance framework to help with risk management which can consist of:
  - Integrated privacy policies
  - Security procedures
  - Data retention procedures
  - Data sharing / vendor agreements
  - Intragroup data transfers
  - Data protection officers' reporting lines and privacy by design
  - Routine audit, training and cultural awareness
- The appointment of key 'data-related roles' to address skills gap shortages and meet the demands of working in the new regulatory landscape.
- Allocating resources and staff training to meet the demands of the new data strategy.

[6] Experian Global Data Management Report, 2017

[7] Ibid



3. "Integrate"

Businesses need to absorb new models of best practice into their data strategy and, ideally, integrate it into the culture of the organisation.

As has always been the case, they need to ensure 'bad data' is prevented from entering their systems after the GDPR deadline has passed. Key contact information should be usable and accurate so that customers can be reached easily. Identity and fraud checks will need to be built into current systems.

Furthermore, organisations will be expected to have the right processes in place to protect their customers in the event of a data breach. Coherent response plans will need to be incorporated into business plans, so that these new criteria can be met.

When assimilating new data-related policies and procedures into your organisation's approach, some steps that should be worked through are as follows:

- Overhaul your data security, especially encryption techniques. Document where any personal data is located and how this is stored. Ensure the data is secure by introducing a culture of data responsibility.
- Introduce a responsive data breach plan allowing you to meet the required 72-hour timeframe. Consider working with external partners to meet the demands of the new rules.
- Build IT systems and procedures that can technically cope with new individuals rights e.g. data portability, the right to be forgotten and enhanced metadata/ record keeping requirements.
- Be prepared to manage data subject rights effectively. Make sure you could cope if the volume of these increased substantially.
- Make sure you can store proof of consent and multiple permissions.
- Evidence your standards and ensure record keeping is embedded into the business going forwards. Put in place relevant policies and documents to support this culture change.
- Privacy by Design and privacy impact assessments should be built in to any new products and services and incorporated into websites, etc, as soon as possible.
- Develop positive privacy communications to enhance transparency and build trust with your customers.

"72 hours – the mandatory data breach notification period under GDPR"

Conclusion:

Thriving in the new regulatory environment

Navigating changing regulation is a significant challenge for businesses. However, appreciating the underlying drivers of new and existing regulations will help organisations understand the rationale behind these developments and improve business outcomes.

The new rules put customers at the heart of business, promoting more transparency and building trust. This can only be a good thing. That said, moving towards a data strategy that allows organisations to flourish in the new regulatory environment is likely to throw up some challenges. Preparation and timely action will be key to making the most of the opportunities ahead.

Those organisations who undertake this due diligence to get in shape for GDPR will be able to forge closer, stronger relationships with customers and improve data strategy. Those opportunities include (but are not limited to):

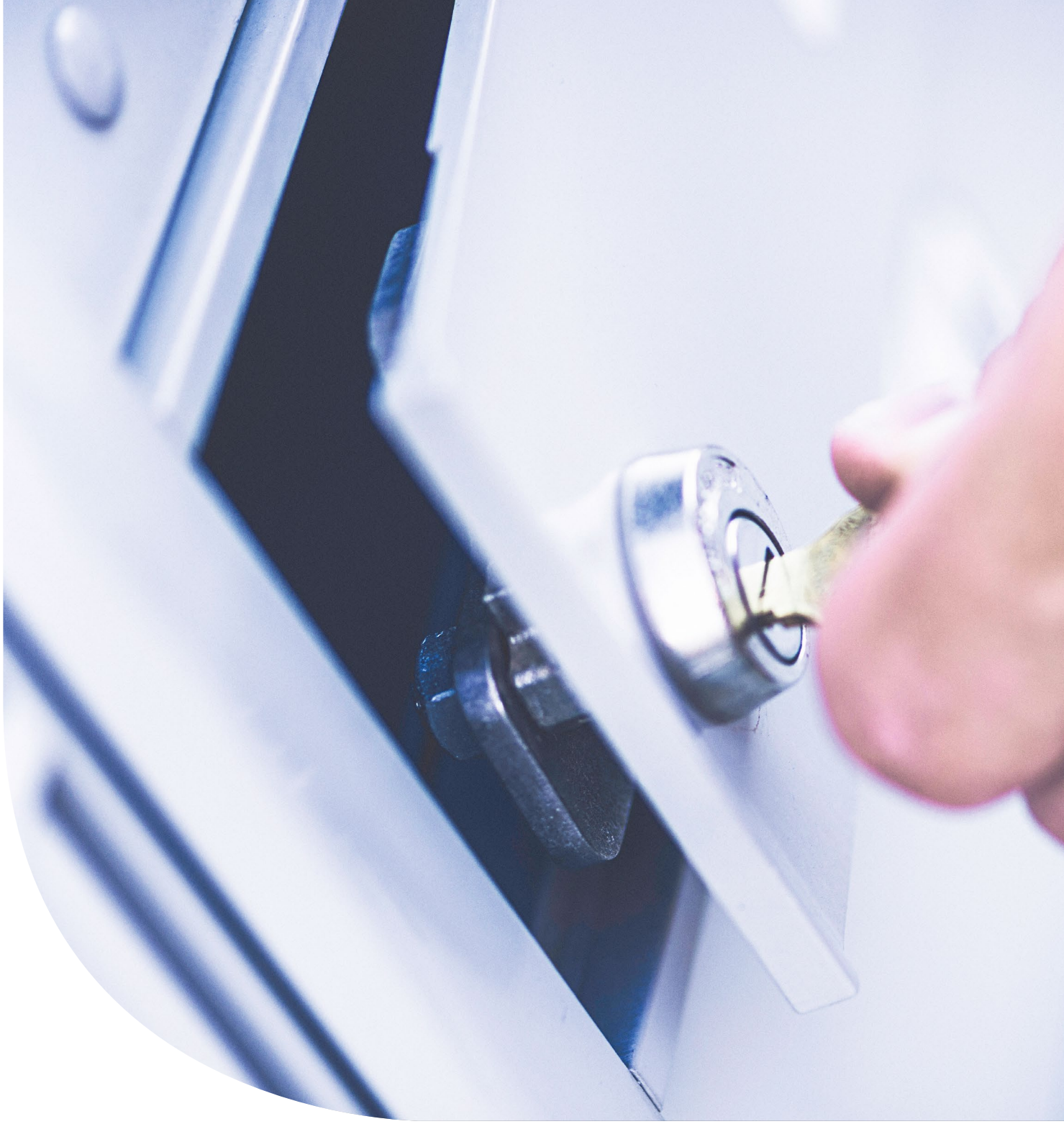
- Working with high quality, better qualified data sets – tighter controls on data gathering will help to increase the quality of your data. Easier consumer opt-out processes will keep the data cleaner and more useful.
- Driving valued and consensual communication – consumers should know exactly what they are signing up to and what they can expect from you, as a result you will be engaging with genuinely interested customers and cutting down on waste.
- Creating targeted and aligned messages and audiences – as you're talking to more engaged and receptive audiences with more targeted messaging, you will see improved ROI as marketing efforts and budgets will be spent on those who are actively engaged with your brand.
- Building trust and advocacy as a brand asset – communicating with individuals who want to hear from you will improve your reputation and provide a better customer experience. As consumers develop trust in an organisation they are prepared to provide more data in order to deliver more value to them e.g. in the form of more targeted advertising, personalised content, and value-add financial services. The GDPR really provides organisations with a clear incentive to create transparency around this value exchange.
- Developing innovation and value for both businesses and consumers – designing services and systems that put the consumer firmly in control and which build privacy and security in, by default.
- The new regulatory environment requires business to really interrogate the way they hold data and think hard about how they use it. First and foremost, the consumer's interests must be upheld.

Providing a privacy notice is an important part of fair processing, and a good first step on the road to transparency. You can't be fair if you are not being honest and open about who you are, and what you are going to do with the personal data you collect. It's important to look beyond the administrative requirements when doing this. Using videos or dashboards, for example, could be one effective way of explaining what you are doing with the data, in a clear consumers-friendly manner.

GDPR is about much more than getting ready for next May – it's for ever. Organisations will go through the next 10 months taking practical steps, such as reviewing policies and notices, appointing a DPO, looking at contracts and international data transfers, getting breach notifications processes in place, looking at data subject rights, mapping data, etc. However, only when they start to think more deeply will they recognise that if they improve their data governance they will achieve a more fundamental and resilient level of compliance.

Although daunting, GDPR should be seen as a chance to transform a business for all the right reasons. Its provisions promise to enforce best practices that can only improve relationships with customers. The challenge is finding an effective way of integrating the new behaviours, processes and roles that are required to be successful, embedding them into the heart of the operation.

Those who live and breathe this new way of doing business, embracing the new standards and focusing on what's right for their customers, will find many chances to prosper in our new data-driven world.



Registered office address:
The Sir John Peace Building, Experian Way,
NG2 Business Park, Nottingham, NG80 1ZZ

T: 0844 4815 888
E: gtmcontactus@experian.com
www.experian.co.uk/gdpr

CM - 518 - 0151

This document is intended as a general guide and not detailed legal or compliance advice