White Paper

Defining the data powered future

An Experian guide to EU GDPR

Foreword

Setting new standards for the digital age

Charles Butterworth, Managing Director, UKI & EMEA, Experian

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.

Introduction

A brief history of EU GDPR

On 28 May 2018, the EU's ambitious General Data Protection Regulation (GDPR) comes into force, by which time all businesses across Europe must comply with the new legislation.

Are you ready? Are you prepared for the new regulations, will you be compliant with the new demands? What impact will the regulations have on your business?

The aim of the GDPR is to strengthen data privacy and protection for all EU citizens. It will transform processes to standardise and protect data and the individual who owns it. The key changes include consumers' 'right to be forgotten' at any point, the right to be informed of data use, and the right to obtain copies of a person's personal data.Despite the publicity surrounding GDPR, and its significance for businesses across Europe, 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.

The need to update data protection regulations has been driven by the proliferation of connected technology. Organisations of all shapes and sizes are now in possession of more customer information than ever before. Current legislation was drawn-up at a time before smart-phones, search engines and social media even existed.

With this explosion of data has come greater responsibility. As the data stack grew inexorably, regulators recognised that existing laws were insufficient to manage how data was being governed. Regulation was needed therefore to keep pace with the rapidly evolving digital landscape both now and in the future.

Following four years' work by the EU, the GDPR comes into force from the end of May 2018. It places enormous responsibility on business as it brings data protection legislation into line with the myriad of ways that personal information has become intertwined in nearly every aspect of our daily lives.

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 Global Data Management Report, 2017

How data management and being GDPR compliant can drive your performance

- Get a clearer view of your customers
- Accurately target new customers
- Deliver an improved customer experience
- Improved business efficiency
- Better customer communication
- Added accountability, credibility and trust

How is personal data regulation changing?

In the 20 years since the EU Data Protection Directive was introduced, countries across Europe have adopted their own local legislation to incorporate it.

At the same time, the world has become digital. We've 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 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. It focuses heavily on protecting individuals and their data. This has also been intentionally agreed as a regulation - rather than another directive - which means it will be a single piece of legislation directly applicable across all EU member states. It includes several new and increased obligations businesses must adhere to.

The role of data in how a company functions will also become clearer, and companies will need to be quick to examine the value of their data and the benefits of keeping it fit for purpose and well protected.

Key elements of GDPR

Although the new legislation amounts to more than 500 pages - these are the key points.

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 elements (Right to Erasure, or Right to be Forgotten) or enhanced (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 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 of data processors
Under the GDPR, data processors will have new 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 are likely to already have many measures in place to demonstrate their 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 regional data protection supervisory authority 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 Fair 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, its value, what it can be used for and are starting to accept the responsibilities that come with this ownership.

Personalisation is one, convenience is another. But when data is collected, it needs to be done as unobtrusively as possible. Even here, there is a data value exchange of sorts – a business that can deliver personalised service, or faster, smarter transactions with a minimum of fuss, will have a significant competitive advantage over its rivals and will be clearly recognised by customers.

Tracking the customer journey is crucial, as is understanding behaviours and preferences - without interrupting on-boarding processes or adding friction to individual transactions. Of course, to win trust businesses must still make sure that their Privacy Policies and Fair Collection Notices are transparent and cover the collection and use of data. But if it's transparent and 'fair' throughout the data exchange, positive customer relationships should be built.

Consumers seem to be increasingly comfortable with sharing their data, on their own terms. A recent Experian survey[2] covering parts of both Europe and North America, 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 wanted.

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

Getting ready for the regulation

It is vital businesses start to think about their implementation requirements now, so as not to risk falling behind. It's all about building relationships and trust.

We can help you. We can quickly **assess your data** for GDPR-readiness, highlight where **improvements** can be made and help ensure you continue to operate a **sustainable** level of data compliance.

Right now, it's not enough to simply feel 'fairly confident' that the data you hold is being used in the interests of the customer. It's a key requirement that new levels of scrutiny are applied and the customer's perspective is at the forefront of whether you are getting it right.

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

ASSESS

Determine data accuracy and overall quality

IMPROVE

Implement an initial **data fix** strategy

SUSTAIN

Extend and embed proactive **data quality management**

[3] Experian Global Data Management Research Report, 2017

Routes to best practice

1. Investigate and assess

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]

[4] Experian Global Data Management Report, 2017

[5] Ibid

- 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.

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, 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. Ensure sustainability

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

The new rules put customers at the heart of the organisation and promote more transparency to help build trust. This can only be a good thing. However, moving towards a data strategy that allows organisations to flourish in the new regulatory environment is likely to create challenges. Preparation and timely action will be key to managing the risk of non-compliance and making the most of your opportunities ahead.

Organisations which undertake this due diligence to get in shape for GDPR will be able to forge closer, stronger relationships with their customers, as well as and improve their data strategy and their business performance.

We can help you by assessing your data and highlighting how and where it can be improved. We can also help you ensure on-going data accuracy through real-time data validation at the point of capture, to help you maintain sustainable regulatory compliance.

Although it may look like a daunting compliance deadline, GDPR should be regarded a chance to transform, optimise and future-proof your business.

GDPR is about much more than getting ready for next May – it's forever.

Denmark
Lyngbyvej 2
2100 Copenhagen
www.experian.dk

France
Tour Ariane
5 place de la Pyramide - La Défense 9
92088 Paris La Défense Cedex
www.experian.fr

Germany
Speditionstraße, 1
40221 Düsseldorf
www.experian.de

Italy
Piazza dell'Indipendenza, 11/b
00185 Roma
www.experian.it

Netherlands
Grote Marktstraat 49
2511 BH, Den Haag
Postbus 13128, 2501 EC, Den Haag
www.experian.nl

Norway
Karenlyst Allè 8B, 0278 Oslo
Postboks 5275, Majorstuen
0303 Oslo
www.experian.no

Russia
5, bldg. 19, Nizhny Susalny lane
105064 Moscow
www.experian.ru.com

South Africa
Ballyoaks Office park
35 Ballyclare Drive
2021 Bryanston, Johannesburg
www.experian.co.za

Spain
Calle Príncipe de Vergara, 132
28002 Madrid
www.experian.es

Turkey
River Plaza
Buyukdere Cad. Bahar Sok.
No: 13 Kat: 8 Levent
34394 Istanbul
www.experian.com.tr

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