TDL | Trust in Digital Life

GDPR for SMEs

Guidance for small and medium-sized businesses on how to approach data protection compliance

A TDL Working Group Publication
October 2018
Version 1.0

Contents

Introduction 3

What you need to know 4

What you should do 5

Data protection by design 6

Checklist 7

Conclusion 8

A GDPR snapshot 9

Introduction

On 25 May 2018, the General Data Protection Regulation (GDPR) came into force which is a significant overhaul of the existing legislation on data protection that was initiated at a time when very few people were using the Internet. The GDPR finally enshrines in law the inalienable rights of individuals to have any data relating to them to be adequately protected and managed, with stiff penalties and fines for companies that do not comply.

If your company is among the many thousands across the EU and beyond that are not aware of the GDPR or the consequences of being non-compliant, then you should read on. Our intention is not to deep dive into the 99 articles of the regulation but to provide an insight into the guiding principles behind them and how a potential compliance nightmare can be turned into a business benefit and advantage.

There are new legislative measures, such as the GDPR, about to have a major impact on businesses that hold data about EU citizens. The massive fines for non-compliance or breach of up to 20 million euros or 4% of global turnover are not, as maybe first thought, red tape for red tape purposes, nor business costs with no commercial objective. On the contrary, the objective of the new legislation is actually to increase customer trust in digital services and thus accelerate technology adoption with all its associated efficiency savings and economic upsides. It also harmonizes data management laws for businesses across Europe, simultaneously reducing medium-term legal costs and facilitating greater pan-European customer engagement opportunities.

Leading up to the introduction of the GDPR in late May 2018, citizens across the European Union were barraged with emails and other communications from retailers, finance institutions, online travel companies, service providers, local government agencies and many, many more. They were all seeking to ensure that customers past and present, consented to the continued storage of their personal information in corporate databases and CRM (customer relationship management) systems and its future use for clearly identified purposes. Behind this activity lay an enormous volume of back office work to review, analyse, validate and systematically cleanse all the accumulated personal data to ensure that what was held on record was there lawfully.

As a consequence, most citizens became at least aware of the existence of the new regulation even if they were not fully cognizant of the details. The same can be said of most businesses and organisations, large and small, the difference being that although larger companies have far more data-bearing systems, they generally have far greater resources to understand, interpret and address what has to be done than do small-to-medium sized businesses.

Despite the apparent general GDPR fatigue that has set in since last May, the regulation has not gone away and is being monitored under the watchful eyes of national data protection authorities in each of the EU Member States, as well as the overarching supervisory body based in Brussels. While there may be a degree of leniency for SMEs, in recognition of the challenges they face in achieving compliance, any honeymoon period will inevitably have to come to an end.

What you need to know

Of the 99 articles and 173 recitals (or legal definitions) in the GDPR, most are open to potential interpretation. Unless you have the time and are prepared to study these in depth, it is unreasonable to expect SMEs to have the resources to grasp all that is required of them. So what gets to the heart of the regulation, the concepts that are key for any business to know and abide by?

Data breach notification

If you are unfortunate enough to have suffered a data breach, you are now obliged to notify the authorities as well as everyone you believe has been affected.

Good news!

There are not many exemptions for SMEs so it is important to highlight one that reduces the burden: SMEs are exempt from doing a record of processing (inventory).

The principles at the core of the GDPR are:

- Empower your customers by informing them - with clarity - about what information you've obtained and what purpose you're going to use it for;
- Show your commitment by providing a user-friendly way for customers to consent and a just as easy mechanism to refuse to your usage of their data, unless your business has a clear legitimate purpose.
- Offer the tools to control and manage that personal data as and when their situation changes;
- Make your customers aware that they can legally challenge your company if your business changes its purpose or use for the personal data (without revised consent), or loses it due to inadequate care.

Customers have the right to:

- Object to their data being used for any marketing
- Full disclosure of how their data will be processed
- Object to their data being automatically processed for profiling purposes
- Full data access
- Require their data to be rectified if inaccurate
- Demand that you erase their data
- Obtain a copy of their data in a form they can take to your competitor (known as 'data portability')

What you should do

Carry out a data audit

Identify all the personal data you're responsible for and find out where it resides. You might be surprised how much you hold.

Identify data processing

Clarify how you process personal data and whether that processing is in line with your legitimate business interests.

- ***Get consent:** if you need that data for business beneficial purposes, you will need to validate that you have explicit consent for that data access and processing.*
- ***Delete and remove:** if not, consider deleting the data and removing those processes.*

Check supplier compliance

If you use third parties to help process the data, and you almost certainly do, audit those suppliers and ask them to confirm their GDPR compliance. You may even need to revise your contracts of service with them in order to indemnify you appropriately. In turn they will undoubtedly require confirmation from you of auditable consent for the data access and processing purpose.

In short, the simple solution is to make your customers' privacy and personal data security your business. Take the 'customer is king' mentality into your digital and online processing and you won't go far wrong. Many individuals are becoming increasingly wary of committing any personal information to the Internet. Some simple steps can be taken by businesses to minimise those risks by adapting your working practices to present a privacy advantage to customers.

Keep it simple, lean and mean

A key principle within the GDPR is data minimization, which means not only ensuring you hold no personal data you don't strictly need, but also that you don't hold it for longer than needed. A breach has consequences for your customer and, if you did not need to hold the data that was breached, expect fines to escalate. Innovative companies will find ways to deliver service with less data and potentially differentiate their offering to prospects on this basis, especially for legally-sensitive data or data considered sensitive by prospects in your industry.

No free lunches

It's amazing how many companies are careless about the third party (especially free) software they use to build websites and generally seek the cheapest Internet service providers, or customer relationship management systems (CRM). Although the more popular content management systems (CMS) are reliably secure, many of the associated plug-ins may not be. 'Free' software rarely comes without a catch – you can be fairly sure the price is extracted in your customer data – so check, because you are now responsible! Cheap services may also use the same techniques, trading price for your business or your customer data.

Business processes

Most of the above is really about business process – not, as most companies tend to think, a responsibility of IT which has a role to play in the validation of suppliers, but in the context of the GDPR its primary role is breach avoidance. IT will also be responsible for detecting and reporting breaches (Do you have tools for that? Many don't). Such reporting goes to the company's nominated data controller who then has to decide whether it needs to be reported to the national supervisory authority for data protection. A collation of minor breaches over time may indicate a systemic failing that needs to be addressed. The supervisory authority expects a log of all internal minor breaches and, if they indicate such a systemic issue, they will expect it to be addressed, especially if it leads to a more serious breach later.

Data protection by design

Public-facing websites.

Many websites have Google Analytics installed without much thought given to the data that collects on visitors.
If you have never made a single decision based on web analytics, you should consider eliminate it.
And while you're at it, review your website's privacy and cookie policies; consider whether the analytics and tracking software (including social media buttons) you employ are worth the trouble to making them GDPR-compliant

With respect to user privacy, the GDPR has attempted to bring into law the seven principles of privacy by design that does not only apply to software development, but also to company processes and procedures. In other words, every SME must have a process to deal with personal data.

Reviewing your company's processes against these principles may help understand how close or far away you are from having the right leadership culture to mitigate risk and maximise business opportunity. If you follow these principles to the letter, you may find little need for consent and your services will have few if any privacy settings. All privacy is contextual – you understand what data you need to process, but does your customer? By finding ways to make it clear to your customers what data you collect and what you do with it, you will mitigate your privacy management challenges.

The seven principles of privacy by design are:

- Proactive not reactive: preventative not remedial
  Take a proactive approach to data protection and anticipate privacy issues and risks before they happen, instead of waiting until it's too late.
- Privacy as the default setting
  Design systems, services and processes to automatically protect personal data. Build privacy into all your company's business practices and customers will learn to trust that their data is adequately protected.
- Privacy embedded into design
  Embed data protection into the design of your systems, services and processes, making privacy part of the core functionality.
- Full functionality – positive- sum, not zero-sum
  Ensure a win-win by ensuring that every system supports privacy and security and there are no unnecessary trade-offs.
- End-to-end security – full lifecycle protection
  Instantiate strong security measures ensuring secure lifecycle management of data from its initial collection to its secure removal.
- Visibility and transparency – keep it open
  Whatever business practice or technology you use should operate according to the stated independently verifiable premises and objectives.
- Respect for user privacy – keep it user-centric
  Keep individuals' interest uppermost in system designs by offering strong privacy defaults, user-friendly controls and appropriate notice.

Checklist

The business rationale comes down to treating data as a quantifiable business asset. The investment required to protect these assets can be compared to an insurance company's approach to providing indemnity to covering home and contents.

SME's can nimbly adapt to the new GDPR in ways corporates are going to find challenging.

This short checklist will help you comply with the GDPR. Being able to answer 'yes' to every question does not guarantee compliance, but it should mean that you are heading in the right direction.

Customer data

- ✓ Do you really need this information about an individual? Do you know what you're going to use it for?
- ✓ Do the people whose information you hold know that you've got it, and are they likely to understand what it will be used for?
- ✓ Are you satisfied the information is being held securely, whether it's on paper or on computer? And what about your website – is it secure?
- ✓ Are you sure the personal information you hold is accurate and up to date?
- ✓ Do you regularly delete or destroy personal information as soon as you have no further need for it?
- ✓ Is access to personal information limited only to those with a strict need to know?

Staff data

- ✓ If you want to put staff details on your website, have you consulted with them about this?
- ✓ If you want to monitor staff, for example by checking their use of email, have you told them about this and explained why?
- ✓ Have you trained my staff in their duties and responsibilities under the GDPR, and do you regularly ensure that they are putting them into practice?
- ✓ If you're asked to pass on personal information, are you and your staff clear when the GDPR allows you to do so?

Policy matters

- ✓ If you use CCTV, is it covered by the GDPR? If so, are you displaying notices telling people why you have CCTV? Are the cameras in the right place, or do they intrude on anyone's privacy?
- ✓ Would you know what to do if one of your employees or individual customers asks for a copy of information you hold about them?
- ✓ Do you have a policy for dealing with data protection issues?
- ✓ Do you need to notify your national information commissioner's office? If you have done already, is your notification up to date, or does it need removing or amending?

Conclusion

Many individuals are becoming increasingly wary of committing any personal information to the Internet, although far too many are oblivious to the risks. Some simple steps that can be taken by businesses to minimise those risks; educate yourself fast and adapt your working practices to present a privacy advantage to customers.

Find out more!

For further practical guidance for companies on how to implement GDPR requirements.

- *The European Data Protection Supervisor (EDPS) the EU's independent data protection authority: https://edps.europa.eu/data-protection/data-protection/reference-library_en*
- *The European Data Protection Board (EDPB): https://edpb.europa.eu/our-work-tools/our-documents_en*
- *The UK Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/*

The GDPR is already having a major impact on businesses, large and small, that hold data about EU citizens. The massive fines for non-compliance or breach of up to 20 MEUR or 4% of global turnover are not, as maybe first thought, red tape for red tape purposes, nor business costs with no commercial objective.

Taking responsibility

No small business can be expected to keep pace with the volume of emerging regulations yet they must do so or risk their livelihood. Every businessman can grasp the importance of having a set of guiding principles and this is just a new set to comprehend and inculcate into company culture. So to make it crystal clear: the management of the new challenge is an executive leadership issue, not one to hand over to marketing, sales or IT.

The privacy paradox

As customers realise their new rights, even if it's only a small number who start querying your systems and processes and raising concerns with the supervisory authorities, the cost to your business could escalate quickly. Embracing the new laws and seeking ways to make it easy for customers demonstrates that you want them to have these new rights, easily accessed and readily understood. If you empower them with control and transparency over the personal data you hold and what you do with it, the rewards come in terms of customer loyalty and trust, whereby they offer more data for more services.

A business opportunity

For dynamic forward-thinking companies embracing the new legislation is a business opportunity. If this is not enticing enough, then it's worth also noting that individuals are going to be massively more empowered by the GDPR with rights over 'their' personal data. If your company abuses or misuses their trust in the way you process their data, then they have new rights to sue or even seek class action lawsuits!

In short, the new legislation is a re-balancing of rights and powers between the individual and the supplier in the digital age. Companies that don't respond rapidly will find themselves left behind by competitors that do or hit with fines or lawsuits large enough to destroy businesses.

A GDPR snapshot

Awareness
Make sure that your staff are aware of the changes to data handling impacted by the GDPR

Information you hold
Document what personal data you hold where it came from and who you share it with - a data audit.

Communicating
Review your current privacy notices and make any necessary changes to align with the GDPR

Customer rights
Check your processes and procedures to make sure they cover all the rights customers have, including how your would delete personal data or provide it in a commonly used format.

Consent
Review your request, record and manage consent to meet the GDPR standards

Customer access requests
Update your procedures to handle requests within the GDPR timelines.

National implementing laws
More than half the EU Member States have enacted laws implementing GDPR and sometimes these laws contain additional requirements.

Lawful basis for processing personal data
Identify and document the lawful basis for your processing of personal information and update your privacy notice accordingly

Children
Consider whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for data processing.

Data breaches
Make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Data protection by design
Check your processes and procedures to make sure they cover your customers' rights, including how your would delete personal data or provide it in a commonly used format.

Data Protection Officer
Designate someone to take responsibility for data protection compliance and their role in your company's governance structure.

International
If you operate in more than one EU Member State, **determine** your lead data protection supervisory authority. If your online business uses non-EU based service providers, you have to ensure they are also GDPR compliant.

trustindigitallife.eu

Trust In Digital Life Association
Maurice Dekeyserlaan 11 / avenue Maurice Dekeyser 11
1090 Jette, Brussels
Belgium

office@trustindigitallife.eu
+44 141 588 0892

TDL | Trust in Digital Life

TDL's vision is that trust must become an intrinsicproperty of any online transaction involving personal information, incorporating legal, business, and technical advances, supporting cyber security policies, and integrating societal considerations so that citizens and end users will recognize trustworthy services, transactions, and data, and be prepared to pay for them. Trustworthy ICT will increase confidence and trust in modern society, bring new and attractive ways of living and working, and further strengthen Europe's democratic and social values.

The association's mission is to provide its members with a European business development platform in order to stimulate development and user acceptance of innovative but practical trustworthy ICT. Guided by its strategic research agenda, TDL acts as an incubator for a portfolio of sprint projects intended to validate new and innovative technology concepts, promotes cross-sector collaboration, and aggregates the results into industry recommendations for policy makers and the European Commission.

trustindigitallife.eu

Trust In Digital Life Association
Maurice Dekeyserlaan 11 / avenue Maurice Dekeyser 11,
1090 Jette, Brussels

office@trustindigitallife.eu
T +44 141 588 0892

TDL | Trust in Digital Life