TDL | Trust in Digital Life

Privacy: the competitive advantage

Guidance and advice for businesses, particularly SMEs, on how to operate in a best practice approach in a privacy-respectful world.

A TDL Working Group Publication
May 2017
Version 1.0

Authors
Geoff Revill, David Goodman

Contents

Digital trust lost

On 25 May 2018, the European Union (EU) will bring into force its General Data Protection Regulation (GDPR) which is a significant overhaul of the existing legislation on data protection that was initiated in 1995, at a time when only a small fraction of the population had heard of the Internet and the founder of Facebook hadn't started High School. 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 you and your company are 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 91-plus articles of the regulation but to give you an insight into the guiding principles behind them and how you can turn a potential compliance nightmare 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.

Issues of customer trust are usually assumed to be a function of the marketing department or sales; or perhaps even of the IT department, if you happen to see digital trust solely through the lens of data security. But if we are honest, when did you last see customer trust as part of a marketing or IT person's job description, let alone have an employee review that qualified or quantified this aspect of their work? This inattention has led to the current status quo where customer data is inadequately protected, and used or shared inappropriately for purposes other than that which the individual originally understood or agreed to.

Numerous studies have shown that trust in digital services is reducing at an alarming rate. People are resorting to tools like ad blockers, or providing inaccurate or obfuscated information upon request. It's a confidence issue – confidence that their data will be protected, that you, the business owner, won't use their information for purposes they don't understand or don't want.

A newly-identified class of digital customers, known as reluctant sharers, arepeople who are concerned about or would prefer not to be, sharing their personal details, but feel compelled to do so in order to gain access to a service or product. However, this growing body of people are potential prospects for dynamic forward-thinking companies that decide to embrace the new legislation as 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.

Reluctant sharers comprise more than 41% of all people online according to the Mobile Ecosystem Forum

New legislation is coming thick and fast. No small business can be expected to keep pace with all this yet they must do so or risk their livelihood. So in this paper we will look behind the law and try to explain the principles that policy makers and strategists are seeking to codify into legislation. 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.

As the balance of empowerment shifts towards the customer, their personal data becomes like money on a company balance sheet, potentially an asset or a liability. Customer data and how it is managed can either contribute business benefits or be a toxic issue that will require expensive attention to remedy if not dealt with. Effective leadership maximises the former and minimizes the latter.

Besides the GDPR, there is another new regulation on privacy (ePrivacy), changes to telecommunications and payments laws (PSD2), new identity management and trust services legislation (eIDAS) and more besides.

The privacy paradox

Reluctant sharers are a strange group. If asked, they'll declare they deeply care about who has their data and what they are doing with it. Yet virtually no one reads a company's privacy policy or takes the time to comprehend what they give away when gaining access to a 'free' online service. This is often referred to as the privacy paradox. Customers want their privacy rights yet have been coerced by current Internet business models to trade convenience over validated trustworthy service. They just cannot be bothered to check. Life is too busy or sometimes it's just seemingly impossible. But, as a consequence of breaches and increasing insight into privacy loss, they are dis-engaging from the digital opportunity. That's not to say digital business is not growing as it replaces traditional methods of doing business, but the untapped growth potential available in a trustworthy digital engagement model has yet to be unlocked.

As customers realise their new rights, expect them to respond. If even a small number start querying your systems and processes and raising concerns with the supervisory authorities, the cost to your business could escalate quickly. What if you embrace the new laws and seek ways to make it easy for customers by demonstrating that you want them to have these new rights, easily accessed and readily understood? In short, if you empower them with control and transparency over the personal data you hold and what you do with it, the rewards in terms of customer loyalty and trust, whereby they offer more data for more services, will be very positive additions to your data balance sheet. While your competitors struggle with the same old sales and marketing or, worse still, an IT-led customer management culture, you'll be sailing away with the market opportunity, unhindered by the burden of worrying about what the new legislation might have in store.

Privacy principles: a trust framework

I considered my data misused when the information I shared was used for a purpose other than that for which I understood it to be provided.

I didn't fully understand how you'd use the personal data you just obtained from me.

The data we exchanged was sold on to multiple parties when I thought it was for a specific purpose within your company.

I'm afraid I don't trust you any more.

Privacy in a digital context is hard to define. It's personal. What's considered private by one person may not be by another. Culture, nationhood, upbringing, religion, morals, ethics, education and more will alter every person's response as to what they consider to be private. Those responses will also vary depending on context.

But what we can agree on is when our privacy is breached: it leads directly to the issue of trust. In a social context trust is an attitude of confident expectation that one's vulnerabilities will not be exploited. But in a business context it's slightly different: an attitude of confidence that a value exchange is fair and equitable.

So in fact trust is enabled by developing confidence in an exchange or engagement. Discovery that one's vulnerabilities were exploited or that an exchange was not fair or equitable undermine trust. Once lost, it's very hard to recover, especially in an Internet of endless easily accessible competitive alternatives.

To gain a prospect or customer's confidence, which over time can evolve into a belief you are a trustworthy supplier, requires a focus on three empowerment principles in the digital exchanges that make up a business relationship: transparency, control and remedy.

Making companies accountable to their customers for the use, care and protection of their personal data is one of the biggest legislative focuses of the GDPR. The new rights individuals have over the access to and use of their personal data under the GDPR serve to demonstrate how a re-balancing of empowerment between business and their customers is being initiated.

While most of these rights place a burden on the business to administer, the last two have perhaps the most impact. If a customer's trust is lost, they can demand to take their data away in a form a competitor can use and they have the right to demand you erase your copy. This would deny you their data as a positive balance sheet item and add it to your competitors! For a minor infraction a customer may just send a warning shot to deny you the right to market to them and, if you don't get the message, escalate that with automated processing restrictions. As you can see, a lot more control is going to be in your customers' hands and so your business needs to sustain customer trust in order to continue to gain the value of their data as part of your business. One should expect that fast-moving GDPR-compliant competitors will ensure prospects are aware of these rights in a sales or marketing process, leaving those who don't keep up with an inability to compete effectively.

The principles at the core of the new GDPR are:

- **Empowering your customers** with clarity about what information you've obtained and for what purpose you're going to use it, with an explicit request to opt in and a just as easy mechanism to opt out, unless your business has a clear legitimate purpose.
- **Offering them the tools** to control and manage that personal data as and when their situation changes;
- **Providing the surety** that if your business changes its purpose or use for the personal data (without revised consent), or loses it due to inadequate care, they can inflict a proportional remedy upon your company.

Customers will have rights 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 ('data portability')

Data on balance sheets

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.

The GDPR shifts the legislative focus from protection of personal data, to a person-centric model with individuals having rights over 'their' data. While the law would not recognise ownership rights over personal data, the concept of the individual owning their data is at the centre of the new legislation. So much so that businesses would be well advised to consider themselves mere temporary custodians of customer personal information, privileged with the rights granted to them by customers to process that information for their profit.

This central concept undermines historic business models for Internet giants such as Facebook, LinkedIn, Google and Apple. In a way that is the strategic opportunity. While traditional US-led business models unfettered by the concepts of personal rights over one's digital life have created the current climate of growing customer distrust, EU companies, backed by EU legislation, can take their regulated and more privacy-respectful business models to market globally as competitive assets. The GDPR only demands you process EU citizen data to its legislative standards, but it would take more effort to downgrade those rights than to offer them globally. In fact, offering a lower grade service to non-EU citizens would limit your business opportunity which would be similar to how US companies respect the constitutional rights of US citizens yet tend to assume that any non-US citizen has no such rights. It lowers trust in US company services and is why US companies are now rushing to place EU citizen data onto servers located in the EU in order to operate fully under EU law. But when you operate under a regulatory framework that extols and ensures the protection of individual rights, you have an asset you can take to market globally.

The regulatory framework can be seen as insurance for individual rights over the access to and processing of their data. Like insurance, legislation gives surety to customers and prospects that the risks they take in sharing their data are indemnified, giving them a remedy if and when data is lost or a business operates inappropriately, and, as with insurance, companies cannot offer these indemnities to their customers unless they operate to a specific standard or they risk a consequential fine of up to €20 million or 4% of global turnover.

Herein lies the last and most important aspect of building trust in a digital customer relationship: the individual's right to a remedy that is centred around them. From the individual's point of view, for example, it makes the consequence of a data breach equitable and consequential on the business. This is the last part of the jigsaw of confidence (re-) building in digital business and, in conjunction with transparency and individual controls, engenders a trustworthy relationship between supplier and consumer.

Personal data that can be deleted by the customer is data that can be taken off your business asset register; data that can have its marketing value rescinded is data devalued on your data balance sheet. Data that is inadequately protected is a major liability on that same balance sheet. Every employee's attitude towards customer data has to be stepped up in order to mitigate the liability risks and maximise the asset value. This is a leadership issue and it's why, under the GDPR, larger companies or those processing sensitive data have to retain the services of a data protection officer (DPO) to effectively work on behalf of their customers. The DPO has to be resourced adequately and, most importantly, report directly to the executive. SMEs that cannot afford this dedicated resource therefore have to take similar responsibilities at the leadership level.

What should I do?

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.

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.

To start with, consider doing 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. Then identify how you process it. Clarify whether that processing is in line with your legitimate business interests and, if not, consider deleting the data and removing those processes. If you still feel you need that data for business beneficial purposes, you will need to validate that you have explicit consent for that data access and processing. If you use third parties to help process the data, and you almost certainly do, you will need to 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.

A key principle within the GDPR is data minimisation. This means not only ensuring you hold no personal data you don't strictly need, but that you don't hold it for longer than needed either. Remember a breach has consequences on 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 sector.

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 CRM tools. Remember '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.

Most of the above is really about business process – not, as most companies tend to think, an IT responsibility. IT has a role to play in the validation of suppliers, of course, 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 have expected it to be addressed, especially if it leads to a more serious breach later.

With respect to user privacy, the GDPR has attempted to bring into law **the seven principles of privacy by design.** 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? Find ways to make it clear to your customers what data you collect and what you do with it, either through the user interface and/or the user experience on your web portal or mobile app and you will mitigate your privacy management challenges. Many aspects of the GDPR look to industry bodies to create guidance frameworks as to what operational practices should be considered default for all businesses. These industry groups will be revising their guidance in light of the GDPR, so work closely with them; or even better get engaged with them to help set the standards yourself. If you operate wildly outside of accepted industry practices, you may find this works against you in the event of a breach assessment fine. If you work within such practices, your customers will have a default level of understanding of what to expect from you, thus minimising your privacy management challenges.

The seven principles of privacy by design are:

- Proactive not reactive: preventative not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – positive- sum, not zero-sum
- End-to-end security – full lifecycle protection
- Visibility and transparency – keep it open
- Respect for user privacy – keep it user-centric

Digital trust regained

Observing the guiding principles behind respectful privacy empowers businesses and citizens and builds trust in the digital world

So by now it should be apparent that something major in the world of privacy is coming soon and, despite the complex and forbidding task of compliance, the guiding principles behind the EU's new GDPR and other related rules and regulations are basic common sense. And, furthermore, the steps that you need to take in your business to align with them are relatively simple to understand and not as onerous as you might have thought to implement.

Making changes in attitudes to your business processes provides a great opportunity to get closer to your customers and to assuage their concerns about how you handle their personal data. If you successfully manage that trust relationship, customers will want to stay with your company and perhaps recommend your business practices to others. All of which adds up to a significant competitive advantage, with the bonus that, by applying the principles of privacy by design, you will not fall foul of the regulatory enforcement agencies and run the risk of incurring a crippling fine.

The sweeping changes that are coming are no longer the domain of sales and marketing, who traditionally have managed customer relationships, or the IT department to install the latest data security patches. Key to making this work for dynamic, forward-thinking companies is having the right kind of leadership that can adapt company culture, its mindset and processes, to the spirit rather than the letter of the new laws. Particularly with SME's, the CEO or a senior executive has to ensure that the right message permeates across the workforce, top to bottom. Succinctly put, that message is: ensure that you have your customers' consent to use their data and make it clear what it is going to be used for. Let them know how long you'd like to hold it for, and, if they ask, where it will be held. And, if one day they want to remove what you have in safe-keeping about them, you will have to give it to them or – worst case scenario – let them hand it over to another supplier. The message also needs to impart that these interactions are not hypothetical or nice-to-have: the consequences for not respecting an individual's privacy, however they perceive it, could be catastrophic financially and damaging to the company brand.

Consumers – a term that, after all, applies to most of us – are being empowered by the new legislation that will come into force over the coming year. Although many may not be aware of the rights they will enjoy, it is only a matter of time before they do. Getting ready before then is vital not only for the health of your business and its data balance sheet but also to persuade hesitant or wary consumers that carrying out transactions online isn't going to result in their identity falling into the wrong hands and create a gaping hole in their finances. It provides the opportunity to restore trust in digital life which both in the short and the long term will be of benefit to everyone in society.

trustindigitallife.eu

Trust In Digital life Association
Aarlenstraat 22 / Rue d'Arlon 22
1050 Elsene, Brussels
Belgium

office@trustindigitallife.eu
T +44 1471 844709

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
Aarlenstraat 22 / Rue d'Arlon 22
1050 Elsene, Brussels
Belgium

office@trustindigitallife.eu
T +44 1471 844709

TDL | Trust in Digital Life