SCALED ACCESS

WHITEPAPER

Data Protection:
From Obligation to Opportunity

Intro

European awareness on data protection is at a steady increase, since the launch of the GDPR, some 2 years ago.

With on-going compliance, GDPR has given out colossal fines to some of the toughest giants on the market and has made online privacy concerns top of mind.

Citizen awareness is reflected in consumer decision-making. Despite the initial re-arrangements and inconveniences that most companies had to endure, it turns out, that Data Protection has not only become an important way to earn trust from customers, but it is in fact a worthy investment in terms of long-term customer satisfaction.

The Cambridge Analytica Scandal Changed the World

Most people would have blissfully ignored the elephant in their rooms for years to come if it wasn't for the eye-opening Cambridge Analytica's data misuse story , the ½ billion phone numbers of Facebook users leakage or the Elasticsearch server personal data breach and more.

A unified and legal mechanism meant to enforce digital privacy and data protection measures to both consumers and organizations was more than required.

The driving element for such a radical approach was the idea that exploiting personal data is not an issue to one or more individuals but a major threat to the EU democracy.

Non-governmental organizations such as NOYB (None of Your Business) and La Quadrature du Net played an important role by preparing the strong and popular legal case for data privacy (which is at the core of GDPR today) and by raising awareness across social media on this topic.

> There is an overwhelming societal desire for transparency on managing and the use of personal data, so the GDPR has superseded anything else.
>
> Laybats, C & Davies, J[1]

And so in May 2018, ahead of the rest of the world, the EU enacts the General Data Protection Regulation, not as mere directive but as fully operating law, carrying a clear and strong message to its member countries: All private and public organizations shall operate *only* with the informed consent of their consumers. Putting consent at the center of GDPR turned a law into a symbol of protection of fundamental civic rights and empowerment over personal data.

From Guiding Principles to Legally Binding

GDPR was not the first initiative of its kind. The EU Data Protection Directive has been available since 1995. The new privacy law relied on the old directive and its basic principles, but it added new definitions and requirements concerning transparency and disclosure to reflect changes in technology which didn't exist before.

Because it was a normative act and not a self-executing law, the Data Protection Directive had a rather guiding role, with no coercive effect to the member states of the EU.

> Privacy is not something that I'm merely entitled to, it's an absolute prerequisite.
>
> Marlon Brando, Actor

[1] Laybats, C., & Davies, J. (2018). GDPR: Implementing the regulations. *Business Information Review*, 35(2), 81-83

Individuals Take Back Control Over their Data

Consent is the core element of the GDPR.

The law requires that it is implemented as a transparent, informed and clearly communicated agreement between consumers and any EU organizations by offering individuals a genuine choice and full control over the processing of their personal data.

The once volatile and often implicit consent process has now become a clear and specific statement of what a data owner is consenting to.

Digital ecosystems in which multiple players access and share multiple resources, now require 3 dimensions of consent: user-to-organization, user-to-user and user-to-application.

The GDPR law not only educates and empowers individuals to control what sort of data they are sharing, but it also encourages them to proactively request that their record is deleted if they deem appropriate.

8 Protection Principles

Consent is not the only element, it is part of the eight GDPR principles that the EU individuals can invoke to protect their privacy and personal data:

1. The right to access - individuals have the right to request access to their personal data and to ask how their data is used by any company, which must provide a copy of the personal data for free.
2. The right to be forgotten - if individuals withdraw their consent from a company to use their personal data, they have the right to have their data deleted.
3. The right to data portability - Individuals have a right to transfer their data from one service provider to another.
4. The right to be informed - individuals must be informed before their data is gathered. Consumers have to opt in for their data to be gathered, and consent must be freely given and NOT implied.
5. The right to have information corrected - individuals can update their data *any time*.
6. The right to restrict processing - *i*ndividuals can request that their data is not used for processing.

7. The right to object- individuals have the right to stop the processing of their data for direct marketing. Any processing must stop as soon as the request is received.
8. The right to be notified – In case of a data breach which compromises an individual's personal data the individual shall be informed of it within 72 hours.

Consumer Awareness? Yes. Still More to be Done

As per Eurobarometer's report back in June 2019[2], 73% of the individuals interviewed heard of at least one of the 8 rights guaranteed by the GDPR.

Interestingly enough, 65% were mostly concerned about the right to access their own data, 61% about the right to update it, 59% the right to object to receiving direct marketing and 57% worried about the right to have their own data deleted.

The results have also shown that data protection remains a concern, with 62% questioning the lack of control over their personal data shared online. We can see that, although great progress has been made in the past year in terms of crowd awareness, there is still more to be done. This may be part of the reason why smaller businesses don't prioritise GDPR compliance as much as they legally should.

89,000 Data Leaks

People across all digital markets started to understand their individual value and are more vigilant about the way their personal data is being used online. Complaints about unwanted marketing and promotional emails, employee privacy, access and account deletion requests and video CCTV surveillance started to pour in.

As per the statistics released by European Data Protection Board[3] in May 2019 after one year since the GDPR was implemented, there have been more than 144,000 privacy related complaints raised by EU citizens and over 89,000 data breaches. Out of these, 63% of these have been closed and 37% were still ongoing at the time the report was issued.

The IntoTheMinds marketing agency collected information from all data protection authorities in almost each EU country. Their study[4] has shown that in 2018 alone,

[2] https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2956
[3] https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en
[4] https://www.intotheminds.com/blog/en/gdpr-statistics-europe/#para52

there was an increase by 86% in complaints related to privacy in data protection, doubling the number of complaints per capita and with Ireland and the UK raising the most of them.

Google Fined for 50 Million Euros

The fact that someone or any organization has the know-how, the tools and the intent to collect and use our personal data in ways we never expect or we disagree with, has finally been acknowledged as a “pivotal privacy concern” although not fully addressed.

However, we see a committed effort from the EU data protection authorities to implement these new privacy rules. Most EU states have adjusted their laws so that any business and legal entity which provides services to the EU, is obliged to be fully compliant with the GDPR requirements, *regardless of whether the data processing takes place in the EU or not*.

A wide range of actions were undertaken by the EU for GDPR infringements during this last two years, from charging hefty fines (up to 20 millions EUR) to imposing a permanent or temporary ban on data processing or suspending data transfers to third countries and restricting erasure of data - all of them having a serious business impact to the organizations concerned.

Protection authorities may impose fines of up to 4% of a company’s annual turnover. They take in consideration various factors before applying a fine, such as the severity, duration and history of the infringement, the type of data involved, the corrective technical and organizational measures taken and so on.

Even so, the total value of fines issued by the end of 2019 was hitting over 400 million EUR and it involved big names such as Google, Marriott International and British Airways (litigations currently in progress). So far, there have been more than 250 fines issued, varying from 100 Eur to 50 million EUR (Google Inc). until 2019.

More recently, another technology company has been fined 150.000 EUR for similar GDPR infringements and in March 2020, Cathay Pacific may be charged with over 500.000 EUR for not properly securing their infrastructure and causing their customer personal data to be exposed.

A quick look at ICO's agenda and coercive actions[5] for this year will make anyone understand how serious the GDPR compliance has become.

> For the first time a European data protection authority is using the possibilities of GDPR to punish clear violations of the law.
>
> Max Schrems, Chairman of NOYB

Cookie Consents

The ePrivacy Regulation (ePR) is seen as an extension of GDPR and it defines how a website or application must manage cookie consents from EU visitors. Companies need to be careful with how they handle consumers' data but they also have to protect their identities across all digital communications. This can mean emails, chats and VoiP calls, push notifications, email marketing and more.

The ePR was initially drafted together with GDPR as a cumulative update to the old privacy directive. It is interesting to know that ePR is an update to Article 7 and GDPR is an update to Article 8, nowhere else but in the EU Charter of Human Rights[6]:

- *Article 7 Respect for private and family life*
- *Article 8 Protection of personal data*

The age at which a person can legally consent to data processing is 16.

The implementation of ePR is currently delayed due to criticism and heavy lobbying from major online media and advertising companies whose most turnover relies on heavy use of cookies[7].

[5] https://ico.org.uk/action-weve-taken/enforcement/
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
[7] https://www.ionos.com/digitalguide/websites/digital-law/eprivacy-regulation-about-the-eus-privacy-policy/

The Ripple Effect of GDPR

> We all know that data is money, and for this reason, businesses have been on a data gathering binge enabled largely by the internet. All that is about to change.
>
> Chris Olson, CEO of The Media Trust

Fueled by the GDPR initiative and its success this past year, similar actions have started to take shape outside the EU. In the US, the California Consumer Privacy Act (CCPA) will become effective in 2020 and it will protect data privacy rights similarly to what the GDPR does.

India's PDPA (Personal Data Protection Act of 2018) has been drafted and Brazil is working on its LGPD law which will enter into effect also in 2020. Several more countries such as Israel, Argentina and even China are working on similar privacy laws and regulations.

We are witnessing a progressive and steady "GDPR-isation" of our laws, digital markets and tech culture. Even major media outlets such as The New York Times[8] are following the example of their EU counterparts and now dedicate time and resources to write extensively on the privacy matter.

Security Brings Trust, Trust Leads to Profit

Companies start realizing more and more how important personal data is to their consumers.

Thanks to the wider awareness arisen through GDPR, expectations have also changed, in the sense that a higher level of trust is now required of businesses in order to keep customers engaged.

To say that PII breaches pave the path toward bankruptcy is as accurate as it can be. A study made by Baringa Partners back in 2018[9] has shown that: *"In the event of a data breach, 30% of people would switch provider immediately and a further 25%*

[8] https://www.nytimes.com/series/new-york-times-privacy-project
[9] https://www.baringa.com/getmedia/f94f0671-ba12-41bd-b664-dc4f54ebf4ac/GDPR-Report-WEB-FINAL/

would wait to see a media response or what others say and do before switching to another provider. It's clear that the majority of customers, by and large, trust businesses with their data. But it's also clear that businesses cannot afford to be complacent..if companies fail to shore up their data defences, it is their brand that will take the hit" - Daniel Golding, Director at Baringa Partners.

AnchorFree ran a survey recently which has shown that 95% of Americans are concerned about businesses collecting and selling their personal information without permission, while 80% were worried about their online privacy and security. Isn't this what a customer thinks of before accessing any online application?

Another significant study, made by Deloitte[10] noted: *"Consumer product executives should consider viewing data privacy and security not just as a risk management issue, but as a potential source of competitive advantage that may be a central component of brand-building and corporate reputation."*

Furthermore, the study notes that *"80% are more likely to purchase from consumer product companies that they believe protect their personal information. 70 % of consumers would be more likely to buy from a consumer product company that was verified by a third party as having the highest standards of data privacy and security."*

Leverage GDPR Compliance for Increased Consumer Trust

In order to sell online products of services, consumers need to access them first. Since ever, companies used any design and marketing strategy available to discourage visitors from spending time reading privacy policies before accessing their website. Too often online applications were designed in ways that endorsed users to consent without proper consideration. Anything was used to make them accept terms quicker: smart layout and text positioning, colorful acceptance buttons vs lengthy documents written in small font and so on.

Although successful at first, the very unethical aspect of these marketing tactics has been invoked in privacy complaints raised by consumers later on.
Companies are now learning that they can leverage GDPR in positive ways.

[10] https://www2.deloitte.com/content/dam/insights/us/articles/consumer-data-privacy-strategies/DUP_970-Building-consumer-trust_MASTER.pdf

A transparent privacy policy showing off improved business practices and security measures re-assures customers that your brand can be trusted. Implementing a simple but efficient consent enforcement solution, covering the full user lifecycle from account creation to deletion and enriched with logs that keeps a history of all user consents (policy versions accepted or rejected, timestamp, region, etc) will resonate the most with customers' privacy needs.

> If you make customers unhappy in the physical world, they might each tell 6 friends. If you make customers unhappy on the Internet, they can reach 6,000 friends.
>
> Jeff Bezos, CEO of Amazon

Conclusion

GDPR is not about compliance, it's about consumer centricity.

By being fully transparent of how they use their data and through implementing mechanisms to appropriately manage PII and prevent data breaches, companies prove that they put their consumers first, who feel valued as individuals and not as mere figures anymore.

So, although GDPR may be challenging at the very beginning, it leverages significant opportunities in terms of engagement and customer retention.

As trust becomes the critical exchange currency at the side of the consumer, seeking to invest in consent and access management technologies specifically designed with GDPR compliance in mind, is desirable and it should become a top priority in the EU organizations and soon enough, across the digital world.