SpyCloud

Everything You Ever Wanted to Know About GDPR in (Relatively) Plain English

With information for companies evaluating SpyCloud

1200 PETABYTES: *The estimated total sum of data held by online storage and service companies like Google, Amazon, Microsoft and Facebook*

Protecting Citizen Data

By now, most industry veterans recognize that the General Data Protection Regulation 2016/679 (GDPR) requires proactive and dramatic change. For EU-based companies, the regulations and implications are a bit clearer than they are in the U.S. and other countries who must comply but still have plenty of questions.

The new data governance regulation was passed on 14 April 2016 and put into effect on 25 May 2018. The regulation was designed, together by the European Parliament, the Council of Europe, and the European Commission, to "protect all EU citizens from the privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the GDPR's predecessor, the 1995 directive, was established."[1]

The older directive referenced is the data protection directive that came into force on 13 December 1995.[2] Officially called the Directive 95/46/EC, it failed to address the modern challenges the world faces when it comes to protecting every citizen's personal data. Today, data is everywhere, living in hyper-virtualized cloud computing environments, on third-party servers, or in a cybercriminal's underground market listing for "fresh fullz."

Experts estimate that the total sum of data held by online storage and service companies like Google, Amazon, Microsoft and Facebook ("the big four") totals more than 1,200 petabytes.[3] That doesn't include other companies like Dropbox. All of this data is quite personal, including PII, financial information, intimate personal photos and conversations most people never considered might be "shared." The EU developed new regulations to attempt to mitigate the consequences of having placed the proverbial cart (the Internet) before the horse (privacy and personal data protection). The primary objectives of the law are to "give control back" to citizens and residents and to simplify the regulatory environment for international business by unifying the regulation within the EU. That's an admirable goal, but why exactly did the EU set out to accomplish this, particularly after similar policies implemented in the past failed?

A Brief History

In 1980, the Organisation for Economic Cooperation and Development (OECD) issued ***Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data***. These were seven unbinding principles suggested to be incorporated into policy governing data privacy protection. The EU incorporated these recommendations into further regulations, including the Data Protection Directive, however, the U.S. did not. Instead, the U.S. endorsed them without implementing them into policy. This may be one reason for the current gap between the EU being more ready to comply with the newer GDPR standards than the U.S.

1 http://www.eugdpr.org/the-regulation.html
2 https://en.wikipedia.org/wiki/Data_Protection_Directive
3 http://www.sciencefocus.com/qa/how-many-terabytes-data-are-internet

The seven recommendations included the following:

1. **Notice** – data subjects should be given notice when their data is being collected;
2. **Purpose** – data should only be used for the purpose stated and not for any other purposes;
3. **Consent** – data should not be disclosed without the data subject's consent;
4. **Security** – collected data should be kept secure from any potential abuses;
5. **Disclosure** – data subjects should be informed as to who is collecting their data;
6. **Access** – data subjects should be allowed to access their data and make corrections to any inaccurate data; and
7. **Accountability** – data subjects should have a method available to them to hold data collectors accountable for not following the above principles.[4]

In 1981, The Council of Europe negotiated The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. This was the first binding international instrument which "protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the transfrontier flow of personal data." It also outlawed the processing of "sensitive" data on a person's race. Finally, it "enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected."[5] The treaty was ratified by all members of the Council of Europe, as well as Mauritius, Senegal and Uruguay.

Meanwhile, the U.S. had ratified no such data protection treaty comparable to those implemented by the EU. U.S. policy on the issue was adopted on a circumstantial basis, such as the passing of the Video Privacy Protection Act of 1988, which was passed after Robert Bork's video rental history was published during his Supreme Court nomination.[6] The Fair Credit Reporting act of 1992 and the Health Insurance Portability and Accountability Act (HIPAA) of 1996 are later examples.

In 2012, the European Commission proposed its intention to consolidate data protection laws in the EU which had been developed by different member states in its "General Data Protection Regulation." These included the consolidation of 27 national data protection regulations into one, the improvement of data transfer policy regarding corporate data transfer to locations outside of the EU, and improvements upon any particular user's control of his or her privacy. This legislation also intended to apply to non-EU companies who would process any data belonging to EU residents.[7] These intentions evolved into what became the GDPR.

4 Shimanek, Anna E. (2001). "Do you Want Milk with those Cookies?: Complying with Safe Harbor Privacy Principles". Journal of Corporation Law. 26 (2): 455, 462–463.

5 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

6 https://en.wikipedia.org/wiki/Robert_Bork_Supreme_Court_nomination

7 https://en.wikipedia.org/wiki/Data_Protection_Directive

GDPR penalties can be quite large: in the case of Mariott, £99 million (£112 million or £123 million.)

What is the GDPR?

Implementation of the General Data Protection Regulation brought with it a number of major changes to existing EU data protection law.[8] A number of these changes are summarized in the following categories:

Increased Territorial Scope (extra-territorial applicability)

The GDPR updates the territorial scope of EU data protection law, which now applies to: (1) companies established within the EU (regardless of whether they are processing EU or non-EU personal data); and (2) companies established outside of the EU which process the personal data of data subjects who are in the EU. In addition, all non-EU businesses processing the data of EU citizens will have to appoint a representative in the EU.

Penalties

The GDPR stipulates two tiers of fines: the first is up to €10 million or 2% of annual global turnover of the previous year, whichever is higher. The second is up to €20 million or 4% of annual turnover of the previous year, whichever is higher. Generally speaking, breaches of controller or processor obligations will be fined within the first tier, and breaches of data subjects' rights and freedoms will result in the higher level fine. And the regulation notes that 'clouds' are not exempt from GDPR enforcement.

As we've now seen in practice, the fines levied can be quite large – for example, in the case of Marriott, the intention to fine £99 million (€112 million or $123 million).[9]

Consent

The standard of consent has been raised by the GDPR. Where relied upon as the legal basis for processing personal data, consent must meet these new stricter requirements.

This stipulation is best communicated directly as it was written:

> *"Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."*

8 http://www.eugdpr.org/key-changes.html
9 https://www.forbes.com/sites/kateoflahertyuk/2019/07/09/marriott-faces-gdpr-fine-of-123-million /#42a0d8db4525

The GDPR also specifies that, *"The request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language."* In other words, consent must be expressed by an opt-in action and data subjects must be informed of exactly what is being used and how, and this can no longer be cloaked by technical jargon or legalese.

Data Protection Officers

'Data Protection Officer' is a new role stipulated by the GDPR, and is responsible for overseeing a company's data protection strategy and its implementation to ensure compliance with the law's requirements. Organisations need not necessarily appoint a DPO unless required to do so by the GDPR. This includes where the organisation's core processing activities consist of the processing of 'special categories of personal data', e.g. health data and/or data relating to ethnicity and race, on a large scale, and/or where the processing activities involve regular and systematic monitoring of data subjects on a large scale. DPOs have to ensure that the data protection rules are respected in cooperation with the relevant Supervisory Authority (SA). An SA is an independent body in charge of monitoring compliance with the GDPR and the processing of personal data within its jurisdiction, providing advice, and hearing citizen complaints.

Controllers are now required to notify local SAs of their data processing activities, which, for multinationals, can present a bureaucratic nightmare, with most member states having different notification requirements.

Data Subject Rights

Breach Notification

Supervisory authority breach notification becomes mandatory in all member states where a data breach is likely to "result in a risk to the rights and freedoms" of individuals. The requirement for notification is only 72 hours. This breach notification requirement extends to affected data subjects where the breach is likely to result in "high risk" to the rights and freedoms of individuals concerned.

Right of Access

Data subjects have the right to request confirmation about whether their personal data is being processed and a copy of such personal data undergoing processing, as well as other information, including the purposes of processing, the categories of personal data concerned and if any third parties have received the data.

Right to Rectification

Data subjects have the right to request that incorrect data stored by an organisation be corrected.

If you're in the U.S. and process data belonging to EU citizens, ***you are obligated to comply with GDPR***

The "Right to Be Forgotten"

This stipulation on data erasure ensures that the data subject has the right to obtain from the controller the erasure of personal data concerning him or her because, for example, the data is no longer relevant to the original purposes for processing, or a data subject withdraws consent.

Data Portability

Subject to certain requirements, data subjects have the right to receive data provided by them to an organisation in a "structured, commonly used and machine-readable format". Data subjects may also request that such data be transferred directly from one controller to another.

Right to Object

In certain situations, data subjects have the right to object to the processing of their personal data, including where the organisation is sending direct marketing communications to the individual or where the data subject rejects the 'legitimate interests' cited by the organisation for processing the personal data.

Privacy by Design

Data protection must be included from the onset of designing systems, rather than as an afterthought. More specifically, protection from the onset of the designing systems, rather than an addition.

What Does This Mean for My Company?

Compliance is not optional

The GDPR is now in effect and all companies inside the EU must comply or face penalties. If you're in the U.S. and process data belonging to EU citizens, you are also obligated to comply.

If you don't comply, it may hurt—a lot

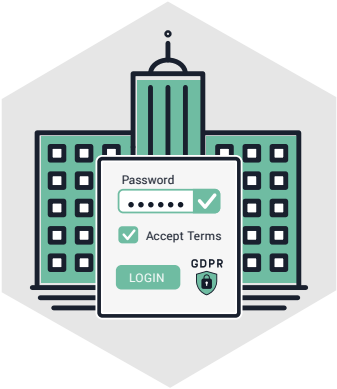
One need look no further than the intention to fine British Airways' £183.4 million ($230 million)[10] for a 2018 breach, where people visiting its website were diverted to a fraudulent site, which harvested details including name, billing address, email address and payment information.

Avoiding significant fines comes down to having adequate data protection measures in place, as well as procedures for identifying and reporting breaches. Blatant disregard for GDPR stipulations won't fly, but making the right investments in protective measures and having an attitude of respecting the law and doing all you can to comply can reduce the fine you'd face if user data is breached.

You are probably not immune

Every organisation must now intimately understand what information they have, who it applies to, if personally identifiable information (PII) of EU citizens is present, and, where and how that information is processed.

10 https://www.cnet.com/news/british-airways-faces-record-breaking-230m-gdpr-fine-for-2018-data-breach/



What *Should* It Mean for My Company?

At the end of the day, compliance with the GDPR goes beyond heeding the right legal advice and taking the best measures to implement recommendations by your counsel. It means doing right by your customers, regardless of where they live, by protecting their personal data and respecting their privacy as you would want other organisations to do for you. It means standing behind the mission statements on your website and marketing materials with more than just advertising, asterisks and deceptively disappointing exceptions spelled out in legalese. As social media becomes smarter, reality becomes augmented, and "sharing" our most intimate information starts to feel like less and less of a choice, maybe it's time to take a hint from The Old World. It certainly can't hurt to follow The Golden Rule now.

GDPR & SpyCloud

SpyCloud is a U.S.-based company with EU clients and one that also processes personal data of EU citizens. Therefore, SpyCloud is required to comply with the GDPR. It's important for our clients to understand how SpyCloud processes personal data under the GDPR and how you can lawfully protect yourself from account takeover (ATO) using SpyCloud without falling foul of the GDPR.

Under the GDPR, before processing personal data, an organisation must establish the 'legal basis' (or combination of 'bases') it relies on to process that personal data.

A key legal basis which can often be relied on is "legitimate interest" i.e. there is a legitimate interest being pursued by the organisation processing the personal data, the processing is necessary for that purpose and the individuals' interests do not override the legitimate interests pursued.

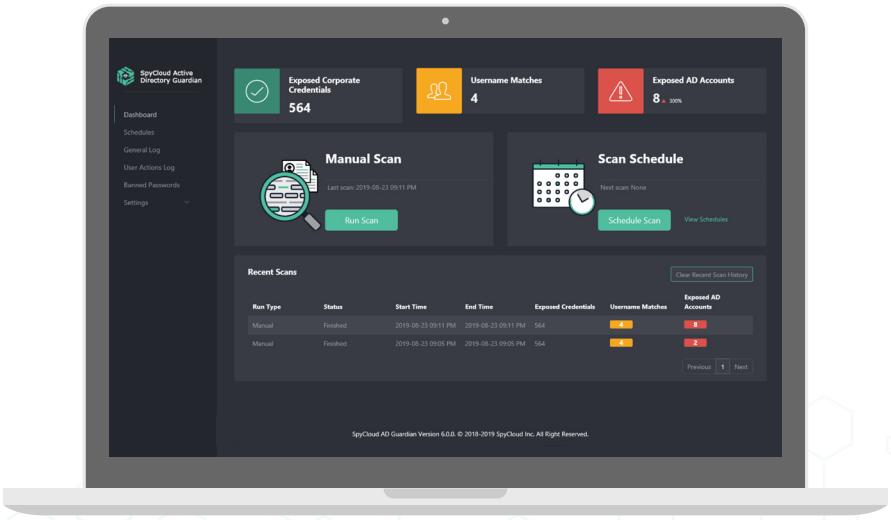


Figure 1: Spycloud's Active Directory Guardian helps to keep your employees' data safe.

Where "legitimate interest" is relied on by SpyCloud, generally speaking, the purpose of the data processing undertaken by SpyCloud is to identify when personal or corporate information of our customers has been exposed to criminal elements. Most of our customers have no idea they have accounts that have been compromised. Using our proprietary software and human intelligence, we are able to identify accounts that are at risk for ATO early in the ATO process alerting clients of a problem and helping customers proactively prevent cybercrime.

Without processing and sharing information in this way with SpyCloud customers, customers are less likely to be able to protect themselves and their employees and consumers from cybercrime.

Our Customers

As a customer of SpyCloud, when you process SpyCloud data, your purpose is to protect your organisation, your users, employees or customers from fraud and cybercrime. With our data, your organisation can proactively protect itself. Keep in mind, when your organisation is alerted of compromised accounts and you take proactive steps to prevent that compromise from leading to ATO, you are also protecting the public. For these reasons, we believe our customers can implement a strong ATO prevention strategy using our services which operates within the law.

Have additional questions about our SpyCloud or our products? Contact us.

SpyCloud