Since the introduction of GDPR back in 2018, it has been more important than ever for businesses to manage the way in which they handle data. However, how has it impacted businesses since it was put into place?

What is GDPR Data Protection?

GDPR or the General Data Protection Regulations applies to all companies that handle and process data in the EU. The aim is to ensure that data protection is strengthened using the correct provisions under the Data Protection Act 1998 and as a result, it has a direct impact on UK law as it is an EU regulation.

The aim of the law is to ensure that online consumers are protected by ensuring they understand their rights when it comes to their data.

What are the implications of the GDPR?

With GDPR firmly in place, it means that consumers now have more control over their data than ever before. As a result, businesses now have to comply with the regulation as the responsibility falls on them to make sure that data is used transparently and safely. Essentially, GDPR is applicable to all businesses within the EU, regardless of whether they handle data or not. Therefore, businesses should have a data protection officer who takes charge of GDPR compliance.

If businesses fail to comply with GDPR then they are likely to face some significant penalties as the fines can amount to 4% of their annual global revenue or 20 million Euros - whichever is the larger.

How does GDPR affect your company?

GDPR has a significant impact on your company because it is especially important for you to manage consumer data in accordance with their expectations and regulations. Therefore, it does have an impact on customer engagement because you have to change many things such as marketing and sales activities. As a result, you will be required to review processes as well as applications and forms to ensure that they are compliant with GDPR.

You have to be able to prove that customers gave consent which means that all data held has to have an audit trail. If you fail to take charge of GDPR then there is every possibility that you will face problems and that could lead to significant problems for your business.

Key Impacts of GDPR on business

As we have mentioned, every business within the EU has to comply with GDPR. What this means is that it is going to have an impact on your business...but what are those impacts? We have covered the main impacts below:

Data Sharing Limitations

Prior to GDPR coming into place, there was less control or governance in relation to the way in which personal data was shared. However, GDPR changed all of this because of the way in which businesses now have to consider how personal data is shared. All of this comes down to consent. If a customer states that they do not want their personal data shared then this cannot be done. Furthermore, they might request at a later date that they don't want data shared and businesses have to be prepared to follow through with these requests and make sure that they comply. Therefore, there are limitations on data sharing which is governed by GDPR.

Improved Cybersecurity

Cyber security has been an issue for businesses since the dawn of the internet and since the adoption of online systems by businesses on a wider scale. It has been an ongoing battle between cyber criminals and businesses to stay ahead of each other. It is an ongoing issue whereby businesses have to constantly update their security across all systems such as infrastructures, end points and networks. This has been something that businesses should be doing or have been doing to ensure that their systems are protected. However, since the introduction of GDPR, security standards have been developed and improved to ensure that the risk of data breaches is significantly reduced. This will ensure that the data of customers is protected as much as possible.

Individual control over personal data

The reality is that GDPR does benefit customers in a way that ensures they are clear about how, when and where their personal data is used. To begin with, they have to give consent about their personal data but it doesn't stop there. At any time, they can make changes to how their data is used and they can even request for it to be deleted or used in a certain way. Where this occurs, businesses have to follow their wishes and ensure that requests are followed accordingly. This individual control over personal data is an integral part of GDPR which is the reason why it is especially important for businesses to ensure that they adhere to the wishes of customers and their personal data.

Non-Compliance Penalties

The penalties that you could face by being non-compliant with GDPR are significant and this has meant that organisations have to consider their responsibilities in relation to data protection. With a potential find of up to 20 million Euros or 4% of your global annual turnover, a simple audit could have a huge impact on your business and that means that it could even face closure if you fail to manage customer data correctly.

Obtaining Informed Consent

Obtaining informed consent is an integral part of GDPR and remaining compliant. Therefore, consent must be an active action that is affirmative and given by the data subject. As a result, it is important for businesses to keep a record of when consent was obtained while remembering that consent can be removed at any time. What this means is that personal data has to be processed in a lawful way and that means that consent is key as people have to be aware of why their data is being processed. There are a range of meanings attached to what makes something 'lawful'. It could be considered lawful if the individual has given their consent but it can also relate to compliance with a legal or contract obligation.

Right to Be Forgotten

As part of Articles 17 of GDPR, the individual has the ability to make a request for all of their personal data to be forgotten and erased without undue delay. As a result, businesses have to ensure that they delete this

data as soon as possible. The right to be forgotten or the right of erasure also relates to reasons why personal data must be deleted should the data no longer meet the intended purposes or if they data subject withdraws their consent. Furthermore, they might also make an objection to the way in which the data was processed or if the data was collected in an illegal way.

Standardisation of Data Protection

GDPR compliance is something that is monitored by each country using their own Data Protection Agencies. Even though independent agencies will undertake these compliance audits, the regulatory environment is standardised across the EU to ensure that once a business has been classed as being compliant with GDPR, it then has the ability to function across all European countries without the need to handle the data protection legislation associated with each country.

The Cost of Compliance

This new regulation has to be managed by businesses. When it was first announced that GDPR would be coming into effect, businesses started putting Data Protection Officers into place. Their role would involve making sure that internal policies were in place and up-to-date and that all necessary processes were put into place. Depending on the volume of data that is being processed by your business, the cost of doing so could amount to tens of thousands of pounds. There is no doubt that GDPR does have some positive implications for businesses as well as consumers, the cost associated with it can grow quickly.

Transparency for consumers

Transparency is vital when it comes to data processing and this begins with obtaining consent as consumers are then aware that their data will be processed. However, businesses are expected to make sure that all forms are concise, intelligible and easy to access when it comes to asking for consumers to agree or disagree with the collection of data and processing. Furthermore, consumers will also be able to understand the reasons for data processing, the different categories that cover the data collected, who will receive the data and how long the data will be stored. Additionally, should there be a data breach, those users who have been impacted must

be informed of the breach as this is a part of GDPR, ensuring consumers are able to take the required precautions.