A MintTwist Guide

The Future of Data Protection

GDPR

minttwist

minttwist

Contents

By Beth Spencer

Welcome the GDPR 3

What is the GDPR? 4

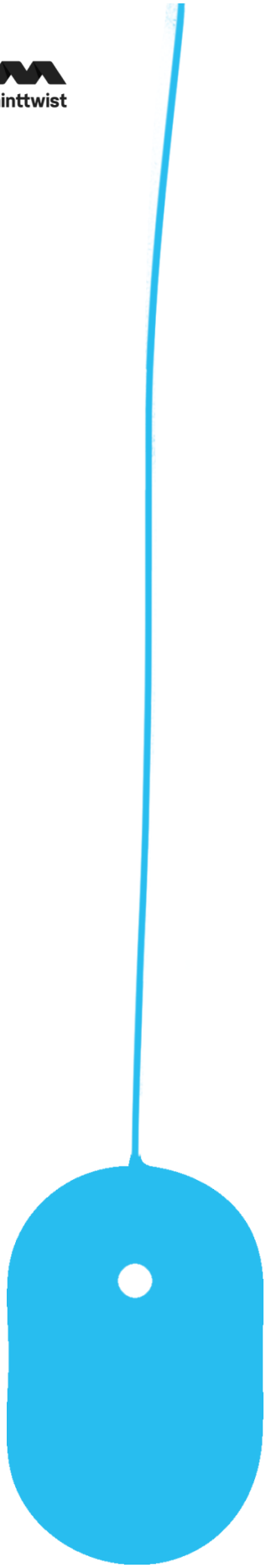
What does the GDPR apply to? 5

How does the GDPR affect your organisation? 6

What should you be doing now in preparation for the GDPR? 7

Summary & conclusion 13/14

minttwist



Welcome the General Data Protection Regulation (GDPR)

As businesses we deal with an enormous amount of our customer's data. Everything from their name(s) and contact details, to payment information and browsing preferences. This data is hugely important to our businesses as it allows us to effectively market our goods and services to customers and improve relations. However, with this comes responsibility. Problems that have arisen in the past include data hacks and leaks. To overcome these issues and to provide the public with more protection comes the arrival of a new data protection law.

minttwist

What is the GDPR?

Coming into force in May 2018 is the new EU data law - GDPR. The arrival of the GDPR represents one of the most important and biggest changes in data protection laws in over 20 years. The GDPR will overhaul existing data protection laws to ensure that organisations are fully compliant, it will increase transparency, improve data governance and make information clearer for individuals to understand.

The GDPR is set to replace the already existing data protection framework of the EU and UK; the Data Protection Directive and Data Protection Act respectively. The UK government have stated that Brexit will not impact on the commencement and implementation of this new regulation.

This new law will come into effect in the UK from the 25 May 2018

minttwist

What does the GDPR apply to?

The GDPR applies to both organisations as well as individuals, such as consumers. For individuals, the GDPR means that the data privacy protection is much clearer and easier to comprehend. Additionally, it outlines to them why organisations need personal information about them.

As for organisations, the GDPR concerns organisations that operate within the EU, and those that operate outside the EU but provide goods and/or services to EU residents. Such organisations must now improve and maintain high levels of protection regarding the data they have collected. They must also obtain explicit consent from the individual before gathering their information.

minttwist

How will the GDPR affect your organisation?

The GDPR will affect your organisation if you obtain and process any personal data of individuals within the EU.

Firstly, the GDPR requires your organisation to operate in a highly transparent manner, and to exhibit accountability and governance. With this your organisation can exhibit such behaviour by obtaining the appropriate, explicit consent from individuals and customers using your service.

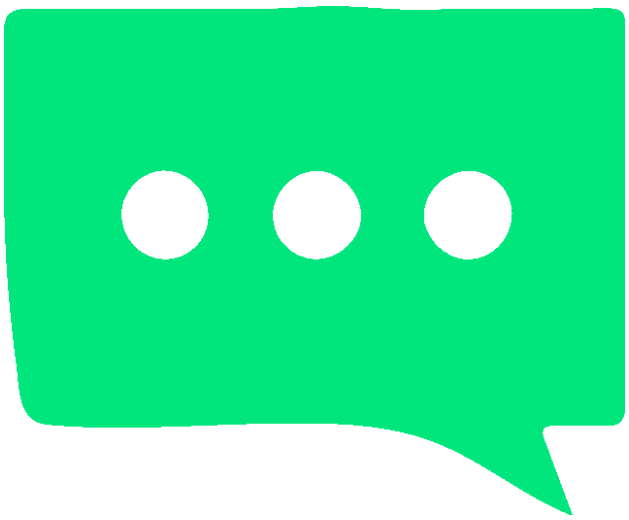
Along with getting explicit consent from people, your organisation will also have to provide them with the right to withdraw their consent. This in turn will impact on your organisation's engagement with customers. For example, it will impact on your email marketing strategy as the individual will have to agree to you emailing them which they may opt out of. Additionally, organisations that use email marketing will have to understand and be evident in the information that they are storing and where it is stored.

As an organisation, you will have to provide evidence that individuals' provided explicit consent to share their personal and sensitive data with you. This means that for all of the data held there must be an audit trail that contains the appropriate information; how they opted in, what they opted into and when they opted in. Due to this it will mean that you have much more information to record and manage correctly.

Another way that the GDPR will affect your organisation is if you experience a security breach, whether due to an accident or cyber-hacking, then you must inform the appropriate people within 72 hours of this happening. This in turn could impact on your organisation's image. However, with the GDPR it encourages your organisation to accept accountability, and improve security flaws thus reducing the threat of data breaches.

If your organisation does not comply with the principles of the GDPR commencing from 25 May 2018 then expect a heavy fine. The fine will be up to €20 million, or 4% of the global annual revenue – whichever is greater.

minttwist



What should you be doing now in preparation for the GDPR?

minttwist

Appoint a data protection officer

You can assign an existing employee of your organisation to take on this responsibility. The role of a data protection officer is to always report to the highest level of supervisor in the organisation, and ensure that the organisation is complying with the GDPR.

The data protection officer must make sure that decision makers and key people within your organisation are aware that the law is changing and the implications of GDPR on the business. Implementing GDPR may have significant resource implications, and it is best to plan those in advance.

Audit all the data you have

If your organisation is already dealing with a lot of data then it is essential that you start to record existing data. This is because as part of the GDPR it is essential that you have an audit of the data you have obtained. The audit should consist of the information that you have about an individual, how they opted in, and what they opted into.

minttwist

Know what the individuals' rights are

As part of the GDPR individuals' have a total of 8 rights that your organisation must comply with. One of the new rights is the 'right to erasure' which means they have the right to withdraw their consent. So, your organisation must ensure that your current procedures and future ones cover all of the individuals' rights.

The eight rights are:

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object, and
- The right not to be subject to automated decision-making including profiling

You may already have these rights already established but it is worth planning for, if for example, someone asks to have their personal data deleted, do your current systems allow you to find this person, delete their data and notify them?

The right to data portability is new and it only applies to information an individual has provided to a controller, where the processing is based on the individual's consent or when processing is carried out by automated needs.

minttwist

Monitor and report breaches

Your organisation should already have existing security infrastructure. You may have to improve upon the security that you already have in place to ensure that it can effectively and efficiently monitor and report data breaches real-time.

Additionally, you may decide to develop security defences in place to contain any data breaches that may occur to protect your data. With this you must also document how your security and protection of personal data complies with the GDPR.

The ICO recommend real-time monitoring because the GDPR states that you must inform the necessary authorities within 72 hours of the breach occurring. Therefore, it is essential that you become aware of such an incident as soon as it happens.

Third party tools and technology providers (e.g. CRM's, Marketing automation platforms etc.) form part of the data ecosystem and it is important that organisations check that their technology suppliers are also prepared for and compliant with GDPR.

Organisations may also need to update third-party vendor agreements that include requirements for the vendor to assist in notifying the regulatory authority if a breach occurs. They must have measures in place to store and process, and integrate data appropriately. We could provide some guidance. It is wise to ask suppliers to detail how they will store / process data to ensure GDPR compliancy. To ensure there is a process in place to manage any data breaches from within the 3rd party tool. And to ensure that it is possible to delete and download data when requested quickly and easily.

Consent

With the GDPR you must provide people with a clear, easy to understand explanation and consent form as to why you want their details. This must be kept separate from other forms. Therefore, it is essential that you update your current consent form to ensure that it complies with the principles of the GDPR.

Consent must be freely given. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions and you will need to include a clear way for people to withdraw their consent.

You are not required to contact all your existing consents in preparation for the GDPR but if you rely on individual's ongoing consent to process their data, it needs to comply with the GDPR standards. If this doesn't currently happen, you need to go back to the individuals and seek a fresh GDPR-compliant consent.

The ‘right to erasure’ clause means an individual can request for you to delete all of the information you have on them. This requires your organisation to also provide a consent form stating that they want the information to be removed, and that you will do so.

Furthermore, you will also have to draft a consent form if your organisation offers a service to children. If the children are under-13 then a parent or guardian signs the consent form.

Update privacy notices

As well as updating your consent forms, you must also update your privacy notices. The information that you should include in the updated version should be why you need their consent for their personal data, and what you intend to use the data for. Additionally, you must also include what your lawful basis for processing their personal is.

Handling Requests

Updating procedures and planning how requests will be handled after new rules have taken place is important. There will not be a charge for complying with a request and you will have a month to comply. If any requests are excessive then you may charge or refuse. Should you refuse a request, an explanation must be given without any delay and given within one month. If many requests are received, then you should consider developing a system to allow individuals to access their information online.

Understand lawful processing of personal data

The GDPR states that you must provide evidence and a reason for your lawful basis on processing personal data. As a result, your organisation must understand what the lawful basis is to process the data you have collected, and record this lawful basis. This data includes name, email address, mobile phone number, bank account details, postal address, credit card number, driver/passport number.

Data protection by design and DPIA

You should consider carrying out a Privacy Impact Assessment and adopt a privacy by design approach. A DPIA is required when data processing could result in high risk to individuals. Examples could include a new technology being deployed or when a profiling operation is likely to affect individuals or when there is processing on a large scale. Data processing is high risk, as indicated by DPIA and if those risks cannot be addressed then the ICO must be consulted to see if the processing operation complies with the GDPR.

minttwist

Summary

Prepare now by raising awareness and understanding of GDPR internally. Make sure that key stakeholders and decision makers in your organisation are aware of the upcoming changes, deadlines and implications.

Assign a Data Protection Officer

Audit and document your data.
Know what personal data your organisation holds/processes, identify where it came from and who you share it with.

Update privacy communications.
Review current privacy policy notices and set plans for any required changes.

Account for individual's rights.
Make sure you have procedures in place that address all the rights that individuals have, from how you would delete personal data to providing data electronically if requested.

Identify your legal basis for processing personal data.
Review and document the types of data processing you conduct.

Put data breach contingency plans in place.

Consider how you obtain consent
How do you currently obtain and record consent? Do you need to amend any processes?

Data Protection Impact Assessments
Make sure you're familiar with ICO's guidance on Privacy Impact Assessments and implement them.

Conclusion

In conclusion, over the next month or two you should ensure that all decision makers and key people within your organisation are aware that the law is changing and start putting in steps to abide by the new regulations.

For further guidance, please call Elliott King or Beth Spencer at MintTwist on 020 3 597 3777.

1-3 Leonard Street
London
EC2A 4AQ

minttwist.com
020 3 587 3777
hello@minttwist.com