What is GDPR and what are its implications?

A guide for businesses

and

professional service practices

EU General Data Protection Regulation (GDPR)

We have compiled this guide to help our customers prepare for the new rules,

which will apply to all organisations from May 2018

This is our interpretation of the regulations and we will update it as we find out more

This guide does not constitute legal advice

Contents

What is GDPR and what are its implications?

The EU General Data Protection Regulation is to strengthen and unify data protection for all individuals within the European Union.

It was adopted on 27 April 2016 and is set to be enforced from 25 May 2018. It will take effect before we leave the EU and it is generally accepted that it will apply even after we leave the EU, indeed in February 2017, Matt Hancock MP, Minister for Digital & Culture, stated that the current plan is to incorporate the GDPR into UK law.

Decision makers and key people need to understand what impact the GDPR will have on their organisation. They need to identify areas that could cause compliance problems.

Which organisations are affected by the GDPR?

It will affect any organisation, whether inside or outside the EU, that holds personal data on EU citizens.

The new regulations affect all companies, organisations, clubs and charities, regardless of size.

Serious breaches will result in fines of up to **€20 million** or **4% of annual global turnover**, whichever is higher.

What is the GDPR definition of Personal Data?

The definition of personal data goes beyond the definition within the Data Protection Act and now includes any records containing a personal identifier. The FAQ page on the http://www.eugdpr.org/gdpr-faqs.html defines personal data as *'any information relating to a natural person or 'Data Subject' that can be used to directly or indirectly identify the person. It can be anything from a name, an ID number, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.'*

Examples of such data are HR records, membership records, contact details including lists of clients, customers, leads, patients and suppliers. The GDPR applies not only to personal data held electronically, but also to manual records.

Fines to make businesses sit up and take notice

Organisations that breach the regulations will face significant fines, certainly enough to harm and possibly be critical for the business.

The fines are daunting with a maximum of €20 million or 4% of annual turnover for the most serious breaches.

Organisations will be fined €10 million or 2% of annual turnover if their records are not in order (article 28), if they do not notify the supervising authority and data subject about a breach, or if they handle 'sensitive data' and have not conducted an impact assessment.

These rules apply to both controllers and processors -- meaning that Cloud Providers will not be exempt from GDPR enforcement.

What is the 'Accountability Principle'

The most significant addition to current legislation is the accountability principle. Companies must understand the risks that they create for others and mitigate those risks. Companies need to build a culture of privacy throughout their entire organisation.

However **small** your business or practice, you must be able to show **how you comply**, not just **that you comply**

What businesses need to do to prepare for GDPR

Data Protection Officer (DPO)

Decide who will take responsibility for data protection compliance within your company and provide training, if required.

Check whether you need to formally designate a Data Protection Officer - not all organisations will need to, although any organisation can do so. Under the GDPR, the appointment of a DPO is mandatory for public authorities and in organisations where the core activities of data controllers and processors are the regular and systematic monitoring of data subjects on a large scale, or of special categories of data, or data relating to criminal convictions and offences.

Whether or not you formally designate a DPO, you need to have sufficient staff and skills to comply with the GDPR.

Identify your lawful right

The next step is to check the regulations in order to identify and document your lawful basis for processing personal data. Article 6 of the GDPR defines lawful reasons. One reason is if you have obtained verifiable, informed and freely given consent.

You may have other lawful reasons **apart** from consent.

In the case of business, a lawful reason would be *'processing is necessary for the performance of a contract with the data subject'* or '*to take steps prior to entering into a contract'*. Other lawful reasons include protecting the vital interests of a data subject (eg awareness of medical conditions) or for compliance with a legal obligation (eg accounting and taxation), or for the legitimate interests of the controller or a third party.

Define your data retention period

Once you have established your lawful right to process data, you will need to define how long you will keep the data for - either a method by which this is determined, or a specific term.

Update your Privacy information

Once you are clear on the above, it is important to update your business's Privacy Policy and Notices. GDPR gives EU citizens (data subjects) the '*right to be informed*' which means that organisations must provide fair processing information in their Privacy Notice and be transparent about how they use personal data.

The potential fine for not doing so is €10 million or 2% of annual global turnover, whichever is higher.

Check whether you need to do a Data Protection Impact Assessment (DPIA)

Preparation of a DPIA is mandatory if you process data that is *'likely to result in high risk to the rights and freedoms of natural persons'*. As an example, it would be required if your organisation carries out evaluation, scoring or profiling of individuals.

The potential fine for not doing so is €10 million or 2% of annual global turnover, whichever is higher.

It is a mistake to think that the GDPR applies only to personal data held in a database . . . it applies to personal information contained, for example, in documents, spreadsheets and recorded phone calls, whether on or off-premises.

Understand the Rights of Individuals

There is a very clear article about individuals' rights on the Information Commissioners Office (ICO) website.

Have you determined how you will you seek, record and manage consent?
Have you a process for dealing with existing data for which you do not have consent?

The process needs to include the provision of a data set to an individual, as well as the deletion of an individual's data from your all of your systems. The question of backups is a complex one that should also be considered.

Find more detail on ICO website

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Document the data handling process

Organisations need to document where they store the data they hold, where it came from, who they share it with and what they do with it.

Organisations that fail to provide this documentation can be fined.

You may need to undertake an audit to identify your sources for data and consent information. Remember to include data that is provided by third parties, such as stakeholders and suppliers.

Obtain Consent for processing personal data

If you need consent in order to process personal data, you must be able to demonstrate that consent was knowingly given by the data subject. Consent cannot be gained from pre-ticked boxes, nor assumed because you have found details that were available in a public space, for example on social media or by picking up a business card.

You may have other lawful reasons **apart** from consent.

When requesting consent, you need to explain the purpose for data processing. Your request must be prominent, specific, in clear and plain language, easy to understand, easily accessible and distinguishable from other matters. It must be as easy to withdraw consent as it is to give it. If you offer services directly to children, you will need to check your additional responsibilities under GDPR.

Be cautious about emailing existing contacts to request consent – there are companies that have been fined for doing so!

Mobile devices and flexible working

Your business data is at risk if anyone in your organisation stores business data on mobile devices such as phones, tablets and laptops, no matter whether these devices are business-owned or user-owned. It is best practice to store all business data on a central server, either on premises or on a private server in a secure datacentre. This enables you to issue passwords so that individuals have access from their mobile devices only to the data that they need on the server. You will have the peace of mind that all the business data is in one place for complete and secure daily automated backup.

Do you need to give your workers guidance regarding using secured connections when accessing the internet?
Can you control and track the data that your staff shares on the internet via Dropbox, Box and similar?

What staff need to know about the GDPR

Anyone who handles personal data has a responsibility to keep it secure and ensure that individual's rights under GDPR are respected. The GDPR makes suggestions on security, which boil down to:

- Ensure that data is secure – with access only to those who need it
- Be able to restore data if you lose it
- Test your security effectiveness regularly
- Encrypt data where appropriate

Staff need to be aware of the significant fines for breaches that would put your business, and thereby their job, at risk.

Data Controllers and Data Processors

Under GDPR, both Data Controllers and Data Processors have statutory obligations and both will be held accountable for compliance.

- If you own or hold data and determine the purposes and means of processing it, you are a Data Controller;
- If you process or store data on behalf of the Controller you are a Data Processor.

Establish who all the Controllers and Processors in your business are - you may need to arrange training if required.

Data Processors can also be third parties, such as Cloud Service Providers that store your data. Third party examples are your online backup, as well as file sharing and syncing via the internet. You need to find out the country where this data is stored.

When to report a data breach

Any data breach that poses a risk to the rights and freedoms of individuals must be reported to the ICO within 72 hours, and in some cases to the individuals affected. See the ICO website. Articles 31 and 32 of the GDPR cover this topic and the Article 29 Working party will produce guidelines in 2017.

Good practice for all staff

- Be aware of and comply with company-defined processes and procedures;
- Be alert to email and phishing scams – beware of clicking on links or opening files sent by unknown sources;
- Use strong passwords and never write them down;
- Never use unsecured public WIFI for accessing or uploading business files;
- Never download personal business data for storage on your mobile device;
- Use a secure file-sharing software in preference to emailing files containing personal data;
- Use only file sharing software that has been approved by your organisation.

If you have shared inaccurate personal data with another organisation, you MUST follow your company's process to inform the other organisation to correct its records. You need to understand what constitutes a data breach and when such a breach must be reported.

Internal business processes that provide GDPR compliance

To ensure compliance with the GDPR's accountability principle, you need to show HOW you comply. This in turn means that you need to be absolutely clear about what personal data your organisation holds, where it came from, whom you share it with. You will also need to maintain records of all data processing activity.

You may want to re-think and change your whole approach to data protection and might use this opportunity to bring about positive outcomes for the business, building trust and improving efficiency. Here is a check list:

- **Identify where personal data is held**
- **Implement procedures to tag and secure the data**
- **The right to be forgotten**: work out how personal data can be deleted if an individual asks for his/her records to be deleted from your systems – and create a policy for deletion of such data from data backups
- **The right to portability**: plan how to handle requests for provision of data sets within GDPR timescales.
- **Have a process to ensure that any new systems are GDPR compliant prior to installation**
- **Consider the ways in which your organisation operates and assess the risk impact**
  - tighten up data security for mobile working – phones, laptops and tablets are frequently lost or stolen and if they hold business data, the business is put at risk;
  - if contractors or employees store or create business files on personal (non-business owned) devices, consider how your company backs up this data and ensures its confidentiality
  - file sharing and/or backup – understand the software that is being used company-wide, if using Cloud services, find out which country is the data stored in, who owns the data, is there an audit trail, does the software include ransomware as standard?
  - cloud apps – how do you record all the apps that your employees use on the devices they use and how will you document what cloud storage are they using

How IT can provide GDPR compliance

To protect against the threat of cyber-attack, businesses need to treat their business data with the same care and attention as their business premises – **Protect, Prevent, Prepare**.

Protect

Equivalent to locking the doors of your building and installing an intruder alarm

- Thoroughly assess all firewall and boundary settings
- Check that there is malware (antivirus) protection on every device owned by the business and ensure that it is robust and up to date
- Ensure that the latest supported version of all software is used and that all necessary patches are applied

Prevent

Equivalent to giving the keys only to those who need access

- Ensure that systems are configured securely and in a way that is appropriate for the business
- Set access codes that allow you to control who has access to your data and at the appropriate level

Prepare

Just as you prepare for total loss of building contents, put measures in place to restore your business data if something goes wrong

- Ensure that daily data backups are taken
- Know who to contact to instigate the restore process and understand how long it will take

5 things that businesses can start right now to improve data security

1. **Plan to achieve Cyber Essentials certification**, the Government-backed scheme that demonstrates to your customers and stakeholders that you are serious about internet security

2. **Use an IT System that is secure by design**
   - encrypted connections between PCs and server
   - role-based access (only see/do what you need)
   - back-end personal data stored in a format that is not easy to read

3. **Share business files securely** and do not use 'grey' file sharing such as personal Dropbox, iCloud, etc

4. **Check your back-ups** – can you restore? Consider automated online backup

5. **Educate your staff to use strong, unique passwords** and to change them when necessary

nTrust Systems – experts in cyber protection for business

We offer

- full-service IT provision covering servers, computers, phone, broadband, email, file sharing, website hosting, data backups and storage
- advice and support to help you achieve Cyber Essentials certification.
- system audits to check for GDPR compliance
- advice and monthly support to ensure GDPR compliance
- remote monitoring of your systems and regular checking for alerts

Cyber Essentials

Advice and support

This is a self-signed security MOT, meaning that at a given time, your IT was secured to a known benchmark standard. Usually there is some work involved in getting things to that standard, and then some more work in keeping people to that standard. nTrust Systems helps businesses achieve Cyber Essentials certification. Cyber Essentials Plus will be a natural progression after Cyber Essentials where organisations identify that further measures are needed.

Read more about Cyber Essentials

Hosted Desktop from nTrust Systems - secure by design

- Employees can use their own devices to securely access data on a central server
- Data is held in a secure Surrey Tier 3+ datacentre
- Connection to the server is secured by SSL encryption
- A hardware firewall limits access
- Data is backed up to two discrete UK locations, so is always available
- Virtual Private Network (VPN) back to your premises if required
- Operating system patches are done overnight
- Software updates are done centrally in one go at times to suit you

Hosted Desktop by nTrust Systems - data safety

- Fully managed off-site IT
- Daily data backup, encrypted at rest and in transit
- Your business data is no longer stored on individual devices, reducing the business risk if those devices fail or are lost or stolen
- nTrust Systems check the anti-virus / malware reports daily and take action if required
- nTrust Systems perform quarterly restore tests

Read about nTrust Hosted Desktop

Call us for our next Hosted Desktop breakfast briefing to see a demo of hosted desktop, followed by Q&A

nTrust Systems – experts in file sharing and syncing for business

nTrust Systems FileCloud

Secure sharing of business files

Businesses will increasingly be required to provide an audit trail for all personal data files that are shared with others.

Businesses should be asking where this shared information is stored and who owns it.

nTrust Systems provides the answers you need . . .
nTrust FileCloud is file 'syncing and sharing' software that gives complete peace of mind – it is a Cloud service on a private UK server with a full audit trail of whom you give access to.

- Data is stored in a highly secure Surrey datacentre and only you own your data
- FileCloud has powerful built-in ransomware protection
- Your data is fully encrypted in storage

Read about FileCloud

When to use data encryption and backup

What is encryption?

Electronic information is changed into a secret code that people cannot understand or use.

When should you use encryption?

Encryption in transit

- Connecting to a server (web, email, remote desktop, file sharing) over a network so that other people on the network cannot see your data.

Encryption at rest

- Backing up data to an online backup
- Syncing data to a file sharing solution

Encrypted devices

- Portable equipment (USB sticks or drives, storage on phones, laptops in general) should probably be encrypted, as they are easy to lose or steal

Encrypted data

- Sensitive data managed by an application should be encrypted, so that it cannot be easily read. It should be difficult for people to deduce the encryption key

Should I encrypt everything to be safe?

If you like, but . . .

- Take professional advice before doing so - it is important to get it right
- If you lose your encryption key, you've lost the data
- If you write the encryption key on a post-it note or the like, then it's no longer a secret code

GDPR Action Checklist

Awareness	Identify and involve key people
Data Protection Officer (DPO)	Appoint someone to be responsible for compliance Act on their guidance
Lawful Basis for Processing Data	Identify why you hold personal data and how long you will hold it for
Accountability	Put on record how you comply with GDPR principles
Privacy Information	What changes need to be made to your Privacy Policy to comply with the GDPR? How will these changes be publicised?
Information	Describe the data and basis for holding it, eg for: • Employees • Customers • Suppliers • Stakeholders Identify data partners: • Who do we get data from? • Who do we send data to?
Individual Rights	Understand the new rights of individuals Ensure Privacy by Design How do you obtain consent? How do you erase records/delete data?
Subject Access Requests	Where do you look for data? How quickly can you respond?
Consent	Do you have clear, opted-in permission to hold and use this data?
Children	Do you hold children's data and, if so, do you understand the new requirements?
Data Breaches	Understand what a breach is Report breaches to the ICO within 72 hours Understand when to report breaches to data subjects
Data Protection by Design	Understand **what** data your systems store Understand **how** your systems store data Understand **where** suppliers' responsibilities end Understand data partners' processes & use of data Fix any identified gaps in your protection of data
International	If you operate in more than one EU state, identify your data protection Supervisory Authority.

About nTrust Systems

Based in Surrey, but operational throughout the south east of England, our offices are adjacent to one of the most secure server hubs in the UK, where we host our Cloud data.

Our business has grown organically since 2002 with a constant stream of referrals from clients appreciating our technical proficiency, sound advice and exceptional service. We are extremely proud of our 98% client retention rate and believe that this fact alone demonstrates why nTrust Systems continues to succeed in a competitive market.

Everyone at nTrust Systems is committed to helping companies get the most from their IT. We offer support packages, hosted desktop services, cyber security advice, VoIP installation and management, website hosting and system analytics.

We insist on a pricing structure which is transparent and fair and we welcome enquiries from businesses of all sizes. Call or email now for an informal chat about your company.

03331 50 60 70 - www.ntrustsystems.co.uk

info@ntrustsystems.co.uk @nTrust_systems

Microsoft Partner
Silver Small and Midmarket Cloud Solutions

nTrust House, 26 Holmethorpe Avenue, Redhill Surrey RH1 2NL

Links

Hyperlinks in this Guide

www.eugdpr.org Definition of personal data
http://www.eugdpr.org/gdpr-faqs.html

GDPR and Accountability – speech by Elizabeth Denham at a lecture for the Institute of Chartered Accountants
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/

GDPR Article 6 - Lawfulness of Processing
https://gdpr-info.eu/art-6-gdpr/

ICO website – Individual's rights
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights

ICO website – Data Breaches
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/breach-notification/

nTrust Systems

https://ntrustsystems.co.uk/cyber-essentials - product leaflet available on this link

https://www.ntrustsystems.co.uk/cloud-services - product leaflet available on this link

https://ntrustsystems.co.uk/FileCloud - product leaflet available on this link

Other links

ICO Website - Key areas to consider
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider/
Esp 6(1)(a) to 6(1)(f)

GDPR: The ICO "12 steps to take now" booklet
https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

Getting ready for GDPR checklist
https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

GDPR
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
GDPR Article 4 - Definitions

Matt Hancock MP questioned on EU data protection rules
https://www.parliament.uk/business/committees/committees-a-z/lords-select/eu-home-affairs-subcommittee/news-parliament-2015/minister-questioned-data-protection/