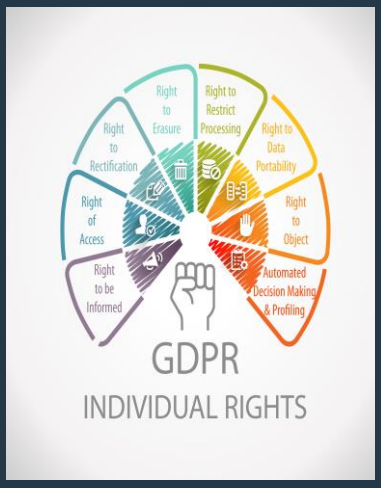
Data Matters
October 2019

What are your individual rights under GDPR?



Right to Rectification

Individuals can have any personal information that is incorrect about them rectified. They can also ask for any incomplete data you hold made complete. Data is inaccurate if it is incorrect or misleading as to any matter of fact.

If you are approached by an individual asking you to rectify their personal data, you are obligated to look into this, they can ask you to do this verbally or in writing.

Data Matters

A big welcome to you all for October's newsletter, the weather is a little cooler since the last newsletter in August. I hope you all had refreshing breaks through the summer, although that feels like a long time ago! I'm sure you are all now busy preparing for the next few months.

It has been a busy couple of months at Apex HR, I have been out on the road, meeting clients, undertaking data audits, supporting and discussing data requirements, and making recommendations around any actions needed to keep data safe.

This month we will be discussing the 'B' word, Brexit, and how this may affect your organisation if we leave the EU without a deal. What are your individual rights under GDPR? We looked at the first and second of the rights last month – this month we will look at the 3rd individual right you have, as an individual, and that you must adhere to within your organisation with clients – the Right to Rectification. We will continue to look at what has changed regarding Data Protection, concentrating on Data Controllers – do you know what the difference is between a Data Controller and a Data Processor?

What is the legal accountability that all Data Controller's must adhere to, to ensure they comply with GDPR?.

We will also look at the work the Information Commissioners Office are undertaking around enforcement action and visits that have taken place to keep personal data safe. And of course, top tips for October.

Preparation for Brexit

Brexit - Where does that leave Data Controllers/Processor in the UK when we leave the EU? Most businesses that operate in the UK may not need to do much to prepare for Data Protection after we leave the EU. GDPR will be incorporated into and form part of the UK's law under the European Union (Withdrawal) Act 2018. The Data Protection Act 2018 will remain in place. Upon leaving the EU, any adjustments to the UK Data Protection Law may mean any policies or documentation you hold could need reviewing and updating, and you will need to ensure that key people within your business are aware of any changes.

What do the ICO say?

The ICO have urged businesses to 'prepare for all scenarios' and published dedicated guidance to help small and medium sized organisations prepare for the increasing possibility that the UK leaves the European Union with no deal on 31 October.

The guidance has been produced to show organisations how to maintain their flows of data.

The sharing of customers', citizens' and employees' personal data between EU member states and the UK is vital for business supply chains to function and also for public authorities to deliver effective public services.

Currently, personal data movement and flow is unrestricted because the UK is an EU member state. In the event of 'no deal', EU law will require additional measures to be put in place when personal data is transferred from the European Economic Area (EEA) to the UK, in order to make them lawful.

If you receive a request to rectify a person's information, you need to be satisfied that the new data you are given is accurate and then rectify their record, if necessary. Take into account any evidence, or discussions you have had with that person.

If the data you hold is potentially inaccurate and used to make significant decisions, about that person or others, you should make a greater effort to rectify the inaccuracy.

You may also take into account any steps you have already taken to verify the accuracy of the data prior to the challenge by the data subject.

You must comply with a request for rectification without undue delay and at the latest within one month of receipt of the request or (if later) within one month of receipt of that person's ID.

If you have disclosed this personal data to others, you must contact each recipient and inform them of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about these recipients.

Apex has a range of packages to assist you with compliance of notices, and the right to be informed. Get in touch for more information.

Your business needs to take crucial steps now to keep your information flowing, such as using pre-approved contract terms (these are currently used to transfer personal information worldwide).

Even if your business doesn't transfer data at an international level, it is still worth reading what the ICO have produced, and make sure you don't need to take any further action.

Please see the guidance below from the ICO, if you need further assistance with these documents, please give us a call to discuss how we can help you be compliant before 31 October.

https://ico.org.uk/dpbrexit/ for small businesses and organisations

https://ico.org.uk/for-organisations/data-protection-and-brexit/

What is the difference between a Data Controller and a Data Processor?

You will have heard of Data Controller and Data Processors, but what does it actually mean?

What is a data controller?

A Data Controller is the person or organization that holds the responsibility of protecting a person's individual rights and privacy. This may be, for example a person using a company website. They also have the control over why and how a person's data is going to be used by them.

A data controller will normally process the data they have collected about a person using their own systems and processes. Sometimes a Data controller will need to work with other outside organisations to process this data.

When this happens, the data controller will always remain in control of that data and specify how it will be used and processed by the outside organization.

What is a data processor?

A data processor will process data that the data controller gives to them on their behalf. The data processor is the outside organisation that the data controller chooses to use and process their data.

Data processes do not own, or control the data given to them by the data controller, meaning that that data processor is not able to change the means or purpose in which that information is used.

Data processors are always bound by the instructions given to them by the data processor.

Keep your personal data safe from hackers and those who wish to make money from ruining your reputation! Encrypt, use malware, lock computers, and keep paper files locked away!

To find out more information about the ICO, visit their website www.ico.org.uk

The activity carried out by the ICO provides support to ensure Data Controllers/Processors are compliant under Data Protection laws.

They will support but they also there to enforce if Data Controllers consistently fail to comply with Data Protection laws and demonstrate Accountability.

The information of Data Controllers/Processors visited by the ICO and their published reports are freely available on their website.

For example:

Company A has a website that collects data about the pages their potential clients may visit, such as the page they enter the site on, how long they stayed on that page for, and what other pages they may have visited. Company A are the Data Controller of this information and, of course, they have a cookie policy and manage consent for this on their web page! Company A also decide how this information they have gathered about usage is going to be processed, used and for what purpose.

Company A uses Google Analytics to find out which pages are the most popular and which are making potential clients leave. This helps Company A to plan what to put on each website page to draw more potential clients into their website.

Company A will need to share the data they receive with Google Analytics to view the insights they need around the success or not of their website. Company A will be the data controller, and Google Analytics will be the data processor.

Companies should look to use a 3rd party data sharing agreement with external companies that they provide data to. This protects the data controller and ensures that the processor has sufficient protection in place to safeguard the data that the Data Controller is ultimately responsible for.

If you are interested in this document, speak to us at Apex HR, where we will be happy to assist you.

Activity carried out by the ICO

The month of August has seen visits to various sites.

These visits have consisted of advisory and audit-based visits from the ICO.

Date of Activity	Identified DC	Type of DC	Type of Visit
7 August 2019	Bupa Health Centres	Health	Audit
7 August 2019	Bupa Care Homes	Health	Audit
7 August 2019	Calderdale & Huddersfield NHS Foundation Trust	Health	Follow up audit
12 August 2019	Dartford & Gravesham NHS Trust	Health	Follow up audit
13 August 2019	Morven Healthcare Ltd	Health	Advisory visit
13 August 2019	Julie West Solicitors	Legal	Advisory visit
16 August 2019	Surrey & Borders Partnership NHS Foundation Trust	Health	Follow up audit
16 August 2019	North Yorkshire Police	Criminal Justice	Audit
23 August 2019	Optima Health	Health	Audit
30 August 2019	Ormiston Academies Trust	Education & Childcare	Audit

The relationship from the Principles to the real life enforcement action…..

As you can see from the enforcement action taken by the ICO how the principles apply and are strictly enforced.

Enforcement Action

A company called Life at Parliament View Ltd were fined £80,000 in July for leaving 18,610 customers' personal data exposed and accessible for almost two years.

Superior Style Home Improvements Ltd were issued with an enforcement notice after making unsolicited marketing calls to individuals registered with the Telephone Preference Service to try and generate UPVC installation leads. The Information Commissioner's Office (ICO) has fined them £150,000 for making nuisance calls.

Hudson Bay Finance Ltd were issued with an enforcement notice for failing to respond to a subject access request.

The ICO continue to carry out advisory and audit visits. These visits are undertaken on a regular basis. Any organization can ask for a visit to take place, to ensure their practices and procedures meet requirements. The audits that are carried out are to ensure the governance and accountability of data processing.
These audit reports are freely available on the ICO website and they are a useful tool to assess and identify areas for improvement and good practice being actioned followed by other Data Controllers and Data Processors.

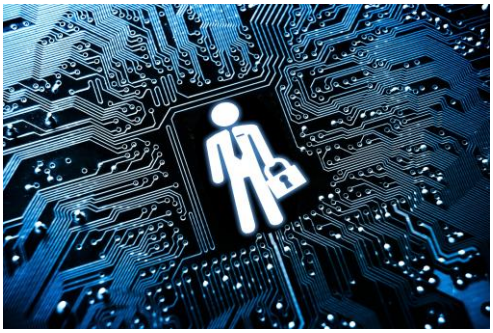
This reinforces the fact the ICO do visit organisations regularly. So, consistently adhering to the Data Protection Act will ensure your organisation remains compliant.

If you feel your company would benefit from a free Data Protection Health Check, please contact Apex HR, where we will be more than happy to help guide you in the right direction. Keeping data safe is all about your companies reputation.

TOP TIP FOR THE MONTH – DID YOU KNOW?

Personal data is about any living individual, but it doesn't have to be private information, even public information already held in the public domain is personal data.
Did you know that the Data Protection Act doesn't cover anonymised information, unless you can identify a living individual from any of the details provided, or by combining this data with other information? If you can identify someone this way, this could still be classed as personal data.

Paper records are only included as personal data, if you are placing this information onto a computer, or if the paper file is held in an organised way (such as a person's HR file). Unfiled papers and notes are exempt from the Data Protection Act.
If you need help with ascertaining what constitutes personal data, and what doesn't, Apex can help.



Changes bought into effect since GDPR was introduced under the new Accountability data protection principle

Data Controllers have the legal accountability to ensure that all personal data is kept secure, that audits have been carried out and that they are fully compliant with the new law. What does this look like? Here are some thoughts for you……

- Your company is responsible for complying with GDPR, and you must be able to evidence your compliance
- Technical and organisational measure should be in place to demonstrate you meet the requirements under the accountability principle
- This includes:
  Ensuring that you have data protection policies in place, and that your staff are following them
- Written contracts should be in place between 3rd party organisations that process any personal data for you
- Evidence and maintain a record of your activities with personal data
- Ensure your data is secured and kept safe, ie. Encryption, locked cabinets
- Recording and reporting any data breaches as necessary to your management team or to the ICO (Governing body)
- Personal data that may be risky to individual's interests should have a data protection impact assessment completed
- Appoint a data protection officer, or someone who will be responsible for data protection within your organisation
- Ensure you adhere to codes of conduct, signing up to certification schemes

These obligations must be reviewed and updated when necessary, make sure you have a privacy culture around personal data across your organisation.
Being accountable builds trust with those doing business with you, and could help you mitigate enforcement action, should it be required

I hope you have found this newsletter interesting, please do let me know if you would like to provide any feedback. Apex has an excellent Data Protection service that can offer you and your company advice and guidance on how to demonstrate your compliance.

So, call or email us at Apex HR and we will support with all of your Data Protection needs.

Check out our Data Protection service on our website.

www.apexhr.co.uk

CONTACT US

Unit 5

Derriford Business Park

Brest Road

Plymouth

PL6 5QZ

01752 825697

info@apexhr.co.uk

www.apexhr.co.uk