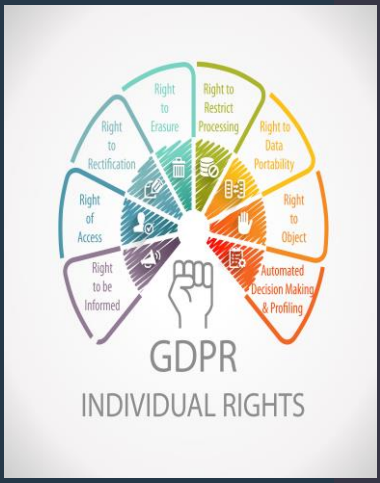
Data Matters
December 2019

What are your individual rights under GDPR?



Right to Erasure

Under GDPR individuals have a right to have personal data erased, also known as 'the right to be forgotten'. It only applies in certain circumstances, which are listed below. A person can request erasure of their records verbally or in writing. You have one month to respond to the request.

Data Matters

A big welcome to you all in December, I am sure you are looking forward to a well deserved break for the Christmas holidays, and hope you all come back refreshed and ready for the New Year in January.

It continues to be busy here at Apex, we are all out meeting some lovely people and undertaking data protection training, data audits and supporting companies to keep their data safe.

This month we will be discussing the new ICO campaign regarding Data Protection fees, the new guidance for special category data and how you should be protecting this within your organisation. What are your individual rights under GDPR? This month we will look at the 4th right – The right to erasure that your organisation must adhere to. We will continue to look at what has changed regarding Data Protection, concentrating on data breaches. Take a peek at the Cyber Security Breaches Survey, which is mentioned in our newsletter. We will also look at the work the Information Commissioners Office are undertaking around visits that have taken place to keep personal data safe. And a top tip for December.

Being near Christmas, we can't not mention the big man in red!

Data Protection Fees

The ICO have launched a campaign this month to contact all registered companies in the UK reminding them of their legal responsibility to pay a data protection fee. This is the beginning of an extensive programme to make sure that the data protection fee is paid by all those who need to pay it.

If you hold any form of personal information for business purposes, including CCTV for crime prevention purposes, it is likely an annual fee is payable. Contact us for more details.

Handling of special category data

A recent blog from the ICO shows why special category data should be handled carefully……

Imagine how you would feel if your medical records, information about your personal life or your political opinions were put into the public arena and anyone could see them?

The effects of information being shared in error can be extremely damaging as well as distressing for the person involved.

The General Data Protection Regulation (GDPR) knows that some types of personal data are very sensitive and states that data controllers must give it extra protection.

This is known as special category data.

People have the right to have their personal data erased if:

the personal data is no longer necessary for the purpose you originally collected or processed it for
you are relying on consent as your lawful basis for holding data, and the individual withdraws their consent
you rely on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
you are processing the personal data for direct marketing purposes and the individual objects to that processing;
you have processed the personal data unlawfully
you have to do it to comply with a legal obligation; or
you have processed the personal data to offer information society services to a child.

You must be absolutely clear with individuals as to what will happen to their data when their erasure request is fulfilled, including in respect of backup systems.

It's good practice to have a policy for recording details of any requests received, especially those made by telephone or in person. You could check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

Special category data is information concerning a person's:

- health;
- sex life or their sexual orientation;
- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs; or
- membership to a trade union.

Special category data also relates to genetic and biometric identification data.

This the most sensitive personal data a controller can process. The misuse of this data could interfere with an individual's fundamental rights and freedoms and cause real harm and damage.

Because of these risks, the ICO expects controllers to take all necessary precautions to protect this data. The ICO have published new guidance to assist with this.

What does the new guidance say about how organisations should approach processing special category data?

Firstly, as always, you must have a GDPR lawful basis to process data under Article 6. However, when processing special category data you also need an Article 9 condition for processing and potentially an associated DPA 2018 Schedule 1 condition.

Many of the DPA 2018 conditions require you to have an appropriate policy document in place. This is a short document that should outline your compliance measures and retention policies with respect to the data you are processing.

There is more work to do when processing special category data, but there are provisions in place to help you protect the data and information of people you hold, which in turn will increase their confidence in you and your company. Take the time to get it right.

Data breaches and their impact

On 3 December a Gloucester local paper stated that the NHS South Central and West team had reported a data breach to the ICO that impacted on thousands of families.

Letters were sent to parents and carers of children aged 3 across the area around Gloucester encouraging them to take up a free flu vaccination at their GP surgery.

A mail merge error meant that the names and addresses of the children were mixed up, resulting in households receiving a letter for the wrong child. The letter provided the name of the child, and no other personal details.

This just proves how easy it is to make an administrative mistake and the huge implications it may have on any company as a result. This could mean an investigation by the ICO and potential fines.

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.

The Cyber Security Breaches Survey for small and micro businesses 2019

- shows some interesting data

31% of micro and small businesses have had cyber attacks in 2018 and continues to cause problems for smaller businesses. Among this 31%:

- 19% lost files or network access
- 10% had their website slowed or taken down
- 9% had software or systems corrupted or damaged.

For the full results to this survey

Visit

www.gov.uk/government/collections

/cyber-security-breaches-survey

Are you confident that the staff within your company will recognise what a data breach looks like?

If you had a breach, would you know what to do?

When GDPR and the new Data Protection Act 2018 came into effect, it became mandatory for companies to report personal data breaches to the governing body, the ICO. (If deemed to be serious enough to do so)

If the breach is severe and affects the rights and freedoms of an individual, this must be reported to the ICO within a 72 hour timeframe.

If it is a low risk breach, you can log, report and deal with this in house, without having to involve the ICO. You should be logging and still investigating these lower risk cases.

In order to be compliant with this part of the act, any company should have a data breach policy, a reporting system, and undertake annual training sessions with staff. Everyone within an organization needs to know what to do in the event of any breach.

If a serious cyber breach occurs, this could also potentially need to be reported to the cyber incident centre.

This is about protecting your company's reputation and being responsible for the precious data you hold about your employees and clients.

If you need assistance to set up data breach systems or training, please get in touch.

Activity carried out by the ICO

The months of September & October have 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
11 September 2019	Glasgow Pregnancy Choices	Health	Advisory
18 September 2019	Homerton University Hospital NHS Foundation Trust	Health	Follow up audit
01 October 2019	South Wales Police	Criminal Justice	Audit
07 October 2019	Optimal Living	Social Care	Advisory
07 October 2019	CAFCASS	Central Government	Audit
10 October 2019	HMRC	Central Government	Audit
10 October 2019	Cambridge University	Education & Childcare	Follow up audit
11 October 2019	TalentEd	Charitable & voluntary	Advisory
17 October 2019	Greater Manchester Mental Health NHS Foundation Trust	Health	Audit

29 October 2019	Northern Ireland health and social care trusts	Health	Overview report
31 October 2019	Northern Education Trust	Education & Healthcare	Audit

The ICO continue to carry out advisory and audit visits. These visits are undertaken on a regular basis. Any organisation 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.

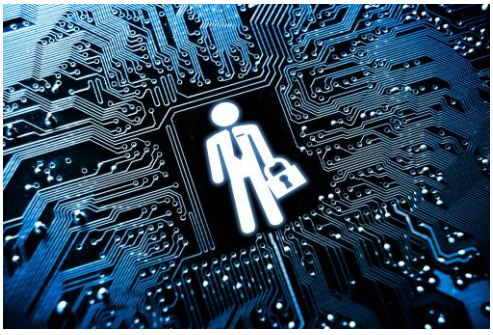
This reinforces the fact the ICO do visit organisations regularly. So, consistently adhering to the Data Protection Act will ensure your organisation remains compliant.

If you feel your company would benefit from a 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 company's reputation.

TOP TIP FOR THE MONTH

Email has many benefits and has changed the way that businesses conduct their affairs. It is also at risk to spam, phishing and hackers. Any conversations and attachments you receive are only as secure as who you send them to.

Fraudsters will attempt to hijack an email address to try and obtain personal information. Be aware of these risks and consider this when sending any personal information. You should always consider if additional encryption should be considered.



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.

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 former Social Services Support Officer at Dorset County Council has been prosecuted for accessing Social Care records without authorisation.

An internal investigation found that the officer had inappropriately accessed the Social Care records without any business need to do so. The records related to four individuals known to the officer.

The officer of Verwood, Dorset, appeared before Poole Magistrates' Court and admitted one offence of unlawfully obtaining personal data, in breach of s170 of the Data Protection Act 2018. She was sentenced to a 6 month conditional discharge, ordered to pay costs of £700 and a victim surcharge of £20.

Contact Us

Unit 5

Derriford Business Park

Brest Road

Plymouth

PL6 5QZ

01752 825697

info@apexhr.co.uk

www.apexhr.co.uk

Finally……..

Public authorities deal with Freedom of Information requests. The Freedom of Information Act runs alongside the Data Protection Act. I thought you would like to see one of the top 10 strangest requests that was received by a local council. Unfortunately, I haven't seen the response provided, but how would you reply?

'What preparations have the council made for an emergency landing of Santa's sleigh this Christmas? Who would be responsible for rescuing Santa? Who would be responsible for rounding up the reindeer, and who would have to tidy the crash site?' (Cheltenham Borough Council)

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.

Kevin Nicola, Lisa and Julie would like to take this opportunity to thank you all for your continued support to Apex and wish you all a Merry Christmas and a happy, healthy New Year.

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