**Data Protection Act 2018**
November 2018

# Data Matters

## Recap on the Principles- Data Protection 2018

In this issue we will recap on the principles and what they mean.

1. Processed fairly, lawfully and in a transparent manner
   ***Lawfulness, Fairness and Transparency***
   Data controllers[DC] and Data processors[DP] aka business', public authorities etc, are expected to make it clear as to why the data is being collected, how it is going to be used, the security of their data, informing them of their rights to their data, ensuring that you are legally entitled to process that data for an intended purpose and not using this data unlawfully or unfairly for other reasons.

2. Collected for specified, explicit and legitimate purpose and not for further processed for other purposes incompatible with the original purpose
   ***Purpose Limitations***
   DC/DP's need to be clear why the data is being collected and what it is being used for. When collecting the data, referring back to principle 1 (transparency), it is important this has been clearly communicated to the person whose data it is via a privacy notice and they have consented. DC/DP's must decide if they are planning to use or disclose the data in addition to or different from the original intended purpose, is fair, lawful and transparent. If the business intends to use the data other than the intended use, it must be compatible, must get the individuals consent for the new purpose.

3. Adequate, relevant and limited to what is necessary in relation to the purposes
   ***Data Minimisation*,**
   DC/DP's must understand that adequate means that you have the sufficient amount of data to properly fulfill why you processed it in the first place; relevant means that there is a lucid link why it was processed and finally limited to what is necessary and that DC/DP's erase the data as soon as possible if not being processed properly. It is important to carefully consider any challenges to the accuracy of the data.

4. Accurate and Kept up to date
   ***Accuracy***
   DC/DP's must ensure that the data processed is up to date and is not misleading, it is essential to maintain the accuracy of the data however this will depend on what it is being use for. If you discover the data is incorrect or misleading, business' have a duty to take steps to correct or erase the data as soon as possible. It is important to carefully consider any challenges to the accuracy of the data.

5. Kept in a form that permits identification no longer than is necessary
   ***Storage Limitations***
   DC/DP's should understand that data must not be kept for longer than it is required, it is important that as a DC/DP's you can justify how long you keep the data. Good practice will be to have a policy setting standard retention period wherever possible. Periodically DC/DP's should review the data you hold and erase or anonymise it when you no longer need it. You must carefully consider any challenges to the retention of the data. In certain circumstances and depending on what the business is involved with, may keep data longer than necessary.

6. Processed in a way that ensures appropriate security of the personal data
   ***Integrity and Confidentiality***
   DC/DP's business' you must ensure that the personal data that is processed has appropriate security measures are in place of that data of which you hold. This protection includes protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or Irganizational measures.

**Let's not forget the 'Accountability Principle', more information was published in our Octobers Newsletter!**

### Examples of Principles…
**(examples taken from the ICO website)**

**Lawfulness, fairness and Transparency.**
Where personal data is collected to assess tax liability or to impose a fine for breaking the speed limit, the information is being used in a way that may cause detriment to the individuals concerned, but the proper use of personal data for these purposes will not be unfair.

**Purpose Limitation**
A GP discloses his patient list to his wife, who runs a travel agency, so that she can offer special holiday deals to patients needing recuperation. Disclosing the information for this purpose would be incompatible with the purposes for which it was obtained.

**Data Minimisation**
A recruitment agency places worker in a variety of jobs. It sends applicants a general questionnaire, which includes specific questions about health conditions that are only relevant to particular manual occupations. It would be irrelevant and excessive to obtain such information from an individual who was applying for an office job.

**Accuracy**
If an individual moves to a new house from London to Manchester a record saying that they currently live in London will obviously be inaccurate. However, a record saying that the individual once lived in London remains accurate, even though they no longer live there.

**Storage Limitation**
An employer should review the personal data it holds about an employee when they leave the organisation's employment. It will need to retain enough data to enable the organisation to deal with, for example, providing references or pension arrangements. However, it should delete personal data that it is unlikely to need again from its records – such as the employee's emergency contact details, previous addresses, or death-in-service beneficiary details

**Integrity and Confidentiality**
The Chief Executive of a medium-sized organisation asks the Director of Resources to ensure that appropriate security measures are in place, and that regular reports are made to the board. The Resources Department takes responsibility for designing and implementing the organisation's security policy, writing procedures for staff to follow, organising staff training, checking whether security measures are actually being adhered to and investigating incidents.

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.

# Activity carried out by the ICO

This month's activity has seen visits to education and childcare facilities and local SME businesses.

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

| Date of Activity | Identified DC | Type of DC | Type of Visit |
|---|---|---|---|
| **13th Nov 2018** | William Henry Smith School | Education & Childcare | Advisory |
| **19th Nov 2018** | West Yorkshire Police | Criminal Justice | Audit |
| **20th Nov 2018** | Roedean Moira House Girls School | Education & Childcare | Advisory |
| **21st Nov2018** | Enquire Learning Trust | Education & Childcare | Audit |
| **23rd Nov 2018** | Harwell Primary School | Education & Childcare | Advisory |
| **23rd Nov 2018** | OCM Business Systems Ltd | General Business | Advisory |
| **23rd Nov 2018** | Barret-Bell Ltd | General Business | Advisory |

The ICO are continuing to carry out advisory and audit visits. From our last issue to this issue you can see that the visits are very regular. 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.

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

From the action taken by the ICO on incidents that have happened, it is clear to see the monetary fines that are imposed to those who do not take Data Protection seriously. Since the update, the fines have increased, in comparison to the fines that have been endorsed recently, future penalties will be greater. This can have a detrimental effect on any organisation who do not take their data protection accountability seriously.

Let's not forget the reputational damage this can also have on the organisations. The ICO enforce action against data controllers who do not take data protection seriously and fail to demonstrate compliance.

# Enforcement Action

## 24th October 2018

The most recent large-scale protection breach, and also made the headlines, is how Uber failed protect customers' personal information during a cyber-attack. There were data security flaws that could have been avoided, which allowed attackers to access a cloud based system. This system held around 2.7millon UK customer personal details, which included names, email addresses and phone numbers. Also, almost 82,000 drivers based in the UK had details of journeys made and money they had been paid taken during the incident. This happened between October and November 2016. Although this happened during this period the people affected by this was not informed until after a year later, instead Uber paid the attackers responsible $100,000 to destroy the data they had downloaded. Needless to say, this was a serious breach of 7 principles of the Data Protection Act 1998 and had the potential to expose customer and drivers to an increased risk of fraud.

*ICO Director of Investigations Steve Eckersley said:*

*"This was not only a serious failure of data security on Uber's part, but a complete disregard for the customers and drivers whose personal information was stolen. At the time, no steps were taken to inform anyone affected by the breach, or to offer help and support. That left them vulnerable.*
*Paying the attackers and then keeping quiet about it afterwards was not, in our view, an appropriate response to the cyber attack.*
*"Although there was no legal duty to report data breaches under the old legislation, Uber's poor data protection practices and subsequent decisions and conduct were likely to have compounded the distress of those affected."*

## 17th May 2018

A former Recruitment Consultant resigned from his former employer and had intentions of setting up his own recruitment business. During his employment he illegally obtained personal information in the form of 272 CV's from his employer's database, he also obtained information relating to clients and service users. In doing so this particular individual was prosecuted at Exeter Magistrates court and admitted the offence of unlawfully obtaining personal data, in breach of section 55 of the Data Protection Act 1998. He was fined £355, ordered to pay a £35 victim surcharge and was also ordered to pay £700 costs.

*Mike Shaw, Criminal Investigations Manager at the ICO, said:*

*"[redacted] thought he could get away with stealing from his old employer to launch his own company. Data Protection laws are there for a reason and the ICO will continue to take action against those who abuse their position."*

## 21st May 2018

The first university to be fined by the ICO under the Data Protection Act 1998 was The University of Greenwich. An investigation was launched and centered around a microsite developed by an academic and student. The ICO found that the university did not have in place appropriate technical and organisation measures to avoid a security breach or ensuring that its system could not be accessed by attackers. Consequently, there was a serious security data breach involving the personal data of nearly 20,000 people, including students and staff. The data included contact details of 19,500 people. Other data details included names, addresses and telephone numbers. 3,500 of this also included sensitive data such as information such as learning difficulties and staff sickness records. The University was fined £120,000 by the ICO for 'serious' security breach.

*Head of Enforcement at the ICO, Steve Eckersley, said:*

*" Whilst the microsite was developed in one of the University's departments without its knowledge, as a data controller it is responsible for the security of data throughout the institution.*
*Students and members of staff had a right to expect that their personal information would be held securely, and this serious breach would have caused significant distress. The nature of the data and the number of people affected have informed our decision to impose this level of fine."*

## 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.*

1. *Lawfulness, fairness and Transparency.*
2. *Purpose Limitation*
3. *Data Minimisation*
4. *Accuracy*
5. *Storage Limitation*
6. *Integrity and Confidentiality*
7. *Accountability*

## Are you registered with the ICO?

*The ICO have started issuing fines to those organisations that have not registered themselves with the ICO. Organisations across the business services, construction and finance sectors are among the first to be fined.*

*The data protection fee followed updates to the Data protection Act 2018, this year on May 25th. Since September, more than 900 notices of intent to fine have been issued by the ICO and more that 100 penalty notice are being issued.*

*To avoid being issued with the above penalty notice, it is in your best interest to register your business with the ICO, depending on the size of your organisation, will determine the fee that requires to be paid.*

*Paul Arnold, Deputy Chief Executive Officer at the ICO, said:*

*"Following numerous attempts to collect the fees via our robust collection process, we are now left with no option but to issue fines to these organisations. They must now pay these fines within 28 days or risk further legal action.*

*"You are breaking the law if you process personal data or are responsible for processing it and do not pay the data protection fee to the ICO. We produce lots of guidance for organisations on our website to help them decide whether they need to pay and how they can do this."*

### What is the ICO Registration?

*"All organisations, companies and sole traders that process personal data must pay the annual fee to the ICO unless they are exempt"*

If you have not registered or have not renewed your registration you could be fined up to a maximum of £4,350.

Find out more about registering on the ICO website,

www.ico.org.uk

## Contact Us

**32 Macadam Road**
**Plymouth**
**PL4 0RU**

**01752 717610**

**info@apexhr.co.uk**
**www.apexhr.co.uk**

Finally, Data Controllers

*Are you able to confidently demonstrate that you adhere to the 7 principles of the Data Protection Law 2018?*

*How do you record your compliance?*

*How confident are you that your staff are aware of the principles and as part of their jobs do they adhere to these principles?*

You no longer have to put off until tomorrow when you can start and act today.

With Apex's help, we have a Data Protection service that can offer you 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**