Data Matters
April 2019

In this edition of Data Matters, Apex would like to welcome to the team Julie Barker.

Julie is our new Data Protection Business Adviser. She will be advising our clients new and existing on their Data Protection compliance in terms of security needs, training, supporting with Data Breaches and Subject Access Requests (SAR). Julie is very experienced and skilled in this area and will be able to support with any business needs. Feel free to drop Julie a line to see how she will be able to support with your data protection requirements.

Her contact details are:

Julie.barker@apexhr.co.uk

Tel 01752 717610

Mob 07855 453415

Data Matters

Welcome to this month's Data Matters Newsletter, which I hope you find interesting and informative. Apex HR follows the ethos of caring for its people first and foremost, people, after all, are what make your business great! Follow this caring outlook with your Data Protection Compliance. 😊

Looking after your company data should never just be a 'tick box exercise'. The data you are responsible for is precious, in life we take great care of things precious to us, like family and friends. Make keeping your data safe a part of your culture, talk about it, be vigilant and challenge decisions. Make sure you take your responsibility seriously, keep your organisation's precious data safe.

We will begin this month by re-capping on clients subscribing or unsubscribing to Marketing.

Recap on Consent for Marketing purposes

In this issue we will firstly recap on your clients subscribing or unsubscribing to Marketing.

The ICO states that 'The Data Subject' must directly opt into marketing, and have the option to opt out, or un-subscribe where appropriate. When looking to market your business, ensure you have followed the steps below

- Check if customers want to be contacted by fax, phone, post or email, and give them the chance to object. You must be able to prove you've done this.
- When you collect customer details, obtain their permission if you want to send them other offers or promotions.
- Ask for their permission if you want to share their information with another organisation.

Letting customers opt out

- Customers have the right to stop their information being used for direct marketing.
- Make it easy for them to opt out - for example by sending a 'STOP' text to a short number or using an 'unsubscribe' link.
- Note in any correspondence, such as a privacy notice, the details of the individual in your organisation nominated to deal with Data Protection, the person they can contact should they wish to opt out of any form of mailing list.

Telesales and Fax Marketing

- You must say who you are when you make a telesales call and give your address or phone number if you're asked for it. The number for customers to call must be a freephone number.
- You're not allowed to send marketing faxes to individuals unless you've received their prior permission, but you can send unsolicited faxes to companies.
- Use the Telephone Preference or Fax Preference Service to see who has asked not to receive calls or faxes

Direct mail

- Check that your mailing lists do not include anyone who's asked not to receive direct mailing, using the mail preference service.

Show you mean business by paying the Data Protection Fee

Paul Arnold, ICO Deputy Chief Executive explains to small businesses why they need to pay the data protection fee.

Businesses that process personal data have to pay a fee to the data protection regulator, the Information Commissioner's Office.

It's the law to pay the fee, which funds the ICO's work, but it also makes good business sense. Because whether or not you've paid the fee could have an impact on your reputation.

When you've paid, your business is published on our register of data controllers. Members of the public and other companies check that list before they decide to do business.

We speak to thousands of people and organisations every week and it's clear that being on the register tells others a lot about you.

It's a strong message for your customers – it lets them know that you value and care about their information and that you're more likely to keep it secure and not share it inappropriately.

It also lets other organisations know that you run a tight ship and that you're aware of your data protection obligations. It indicates that you're more likely to take your other data protection responsibilities seriously too. It's a reassurance for those thinking of doing business with you.

For most organisations, the fee is either £40 or £60 a year depending on your turnover and how many people you employ.

If you're not sure whether you need to pay, you can check on the ICO Website.

There's another good business reason to pay too. If you need to pay and don't you will be fined. Fines range from £400 to £4,000 and since May, when the current law came into effect, we've issued 103 penalty notices to companies for failing to pay.

E-mail marketing and text messages

- You're only allowed to send marketing emails to individual customers if they've given you permission.

Emails or text messages must clearly indicate:

- who you are
- that you're selling something
- what the promotions are, and any conditions

Check that you are not sending emails to anyone who's asked not to receive them, using the Email preference service.

- If you buy or rent a mailing list, ask the supplier if you have the right to use it for email marketing.
- Every marketing email you send must give the person the ability to opt out of (or 'unsubscribe from') further emails.
- You must tell customers if you add them to a list of people who do not want to be emailed.

Cookies

- You must tell visitors to your website how your site uses cookies and also ask if they want to accept them. The information should be easy to understand.
- Find out more about cookies on the Information Commissioner's Office website and AboutCookies.org.
-

Remember:
You must be able to prove that you've checked you're not contacting anyone who does not want to be contacted.

Did you know? It's illegal to phone or fax someone registered with these services if you do not have their permission. You can be fined up to £500,000 for each unsolicited phone call.

Remember - Customers can complain if you misuse their information, and you could be ordered to pay a fine or compensation.

Activity carried out by the ICO

This month's activity has seen visits to various sites including education and childcare facilities, the public sector, charities and private 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
05 April 2019	St Josephs College, Reading	Education & Childcare	Advisory
05 April 2019	Polish Saturday School in Darlington	Education & Childcare	Advisory
05 April 2019	Durham Johnston School	Education & Childcare	Advisory
02 April 2019	Total Communication	Charitable & voluntary	Advisory
29 March 2019	James McKenzie (Wills) Ltd	Legal	Advisory
28 March 2019	North Norfolk Academy Trust	Education & Childcare	Audit

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.

26 March 2019	Delta Academies Trust	Education & Childcare	Audit
22 March 2019	Spring House Medical Centre	Health	Advisory
22 March 2019	North West Ambulance Services NHS Trust	Health	Audit
15 March 2019	Hampshire Office of the Police & Crime Commissioner	Criminal Justice	Audit

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

If you consistently adhere to the Data Protection Act will ensure your organisation remains compliant. To help you address this, Apex HR can offer you a free no-obligation Data Protection Health Check. This can help you understand the levels of compliance within your company, and, more importantly, ensure that your personal data is being taken care of. Contact Julie for more details, who will be more than happy to assist.

Enforcement Action taken by the Information Commissioner's Office

- The Information Commissioner's Office (ICO) has fined Vote Leave Limited, £40,000 for sending out thousands of unsolicited text messages in the run up to the 2016 EU referendum.

  An ICO investigation found that Vote Leave sent 196,154 text messages promoting the aims of the Leave campaign with the majority containing a link to its website.

  The investigation also found that Vote Leave was unable to provide evidence that the people who received the messages had given their consent; a key requirement of electronic marketing law.

- A Kent pensions company which relied on 'misleading' professional advice has been fined £40,000 by the Information Commissioner's Office for being responsible for sending nearly two million direct marketing emails without consent.

- The ICO fined Bounty (UK) Ltd £400,000 for illegally sharing personal information belonging to more than 14 million people. Their investigation found that Bounty, the pregnancy and parenting club, collected personal data for

membership registration through it's website and app, merchandise pack cards and directly from new mothers at hospital bedsides.

But, the company also operated as a data broking service until 30 April 2018, supplying data to third parties for electronic direct marketing. The company shared approximately 34.4 million records between June 2017 and April 2018 with credit reference and marketing agencies, including Acxion, Equifax, Indicida and Sky. These organisations were the four largest recipients out of a total of 39 organisations which Bounty confirmed it shared personal data with.

The personal data shared was not only of potentially vulnerable, now mothers or mothers-to-be but also of very young children. The investigation found that for online registrations, the privacy notices had a reasonably clear description of the organisations they might share information with, but none of the four largest recipients were listed. None of the merchandise pack claim cards and offline registration methods had an opt-in for marketing purposes.

Steve Eckersley – the ICO Director of Investigations said,' Such careless data sharing is likely to have caused distress to many people, since they did not know that their personal information was being shared multiple times with so many organisations, including information about their pregnancy status and their children'

Keep your Data Safe – Top Tip for the month

Think also about how you physically hold data – Do you shred confidential waste and keep your desks clear, or could someone walk in off the street and access the data you hold? Could someone break into your office and take an unencrypted laptop or hard drive that contains sensitive data? Do you send personal data in the post, is it sent via recorded delivery, or hand delivered.? Making small changes to your current processes can ensure your data is kept safe, and in the right hands

Recent Cyber Attack in Bridport

A school in Bridport made the news in March when they experienced a cyber attack on their systems. The Sir John Colfox Academy said a member of staff mistakenly opened an email containing a virus. Hackers used ransomware to encrypt files at a school, causing it to lose some students' GCSE coursework.

The email claimed to be from a colleague at another Dorset school and infected the computer network. Coursework from one subject submitted by Year 11 students, which was saved on the school system, has been lost.

Hackers will always find new and innovative ways to infect machines, and so-called ransomware has become one of the most popular ways for cyber criminals to make money. In a typical attack, malicious software is installed on a victim's computer - typically via a link that is sent in an email - and will then proceed to encrypt all the files on it. To get the data back, the victim will be asked to pay a ransom, often in cryptocurrency, within a certain timeframe. Unfortunately, schools and other public institutions, such as hospitals, have become regular victims, because hackers think they will be less likely to have good cyber-practices. Falling victim can be hugely damaging to reputation - and a school which has lost GCSE coursework as a result of an attack will have some explaining to do to parents and pupils.

All of this could be simply avoided with some straightforward steps.

- Backing-up data on an external drive
- Keeping anti-virus software up to date
- Educating anyone who uses the network to not open unsolicited emails or click on suspicious links.

https://www.senseon.io/partner/bruce-brooker

Contact Us

32 Macadam Road

Plymouth

PL4 0RU

01752 717610

info@apexhr.co.uk

www.apexhr.co.uk

Last week school leaders were urged by the government to take action after a "significant increase" in cyber attacks on academy trusts were recorded.

How can you keep your electronic data safe?

We spoke to one of our trusted associates **Bruce Brooker from Senseon**, who provides Cyber defence. Senseon was named in March by Techworld as the 'UK's top cyber security start up'. Senseon's automated investigation accurately detects and understands cyber threats, saving you time and resource.

If this is something that may appeal to you or your organisation, please get in touch with Bruce for your free trial, details as below. **As food for thought……**

- 7 million cybercrimes are committed against smaller businesses in the UK every year
- 19,000 cybercrimes committed each day
- Cyber criminals are foremost concerned with increasing their financial gain. They seek to do this by stealing private financial information, personal details and account log in credentials, so that they can go on to commit fraud, data theft of extortion
- Some hackers use fake email accounts to trick employees into sending huge amounts of funds to a bank account owned by the cyber criminal
- Cyber attack tactics include:
- Malware
- Distribution Denial of Services Attacks
- Ransomware
- Phishing Emails

For further details and to register for a free no obligation trial of the technology please click on the link below to complete your details:

https://www.senseon.io/partner/bruce-brooker

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