SPA Newsletter

...Strength in Numbers

Welcome

to the April 2018 SPA newsletter

Special AGM and GDPR Edition

SPA AGM 2018 20 June 2018 at historic Hatfield House

Our AGM this year will take place at Hatfield House, where Elizabeth I spent much of her youth.

It's a beautiful setting, with good accommodation for both the AGM and the other activities which will happen as usual in the morning.

There will be lunch and, in the afternoon, tours of the house, and plenty of time to visit the grounds. There is ample parking.

As last year, there will be no charge for the event.

You should have received your invitation by now. If not please call Jacob at SPA

TIMETABLE

9.30	Arrive at the Hatfield House – Riding School for tea, coffee and biscuits
10.00	10.00 AGM and CPD in the Riding School / for guests ceramic painting at Pots of Art
12.00	CPD question time
12.45	Lunch in the Old Palace – magnificent 15th Century Elizabethan Hall
14.30	Tour of Hatfield House
	Visit attractions

CPD

The CPD Session will be provided by speakers from Croner Taxwise and will cover

- GDPR
- Tax update
- Capital allowances and R&D
- Other practice topics e.g. the more common sources of PI claims and some HR issues

The SPA Steering Committee needs new blood

We need your help to develop the services which SPA offers to its members. Please contact Howard or any of the steering committee, if you would be interested in joining us.

GDPR - How does it affect me? What do I need to do?

We all know GDPR (General Data Protection Regulation) is supposed to come into effect on 25 May 2018, and that there are a number of scare stories out there, but things are now beginning to settle down. What follows is our take on what you need to do. However, the legislation has not yet been passed into UK law, and we, along with everyone else, are feeling our way a bit on this.

1. Have a plan

This is the only thing you really must have in place by 25 May - a plan, in writing, to deal with the challenges of GDPR. The following steps and the attached checklist are designed to help you draft that plan.

If you think there are things we haven't thought of - we would love to hear from you.

We have tried to write this in plain English, but again, if anything is unclear, we would love to hear from you.

2. Appoint a data controller

If you're a sole practitioner it would be you - if you're in partnership, best not to leave the office, go on holiday or maternity leave, or your partner(s) will decide it's you.

Under the current rules, on the assumption that you are already registered with the ICO, this will represent no change.

3. Establish whether you hold personal data

If you have employees, if you have personal clients - you do.

NB GDPR applies to personal data only, not data on businesses or other entities.

4. Establish how you will gain the necessary permissions

If you have personal data to enable you to provide your services to your clients or to pay salaries to your employees, it is lawful for you to hold and process that data. For any other reasons - marketing, PR etc. you need to obtain permission from the person concerned and they have to "opt in" - you can't just have a default assumption that they agree. So no pre-ticked boxes on forms or web pages.

Also, be aware that when an employee or client becomes an ex-employee or ex-client the relationship with them changes. It may well be that holding their data remains lawful because there may be statutory reasons for you to hold it, but there may not.

5. Access and Transparency

Although it may well be lawful for you to hold personal data, the people concerned - "data subjects" - have rights of access to that data to ensure that it is correct, that it is all necessary for the intended purpose and that it is not being held for an unnecessarily long period. So you have to enable them to have access if they request it, and you have to inform them of their rights of access.

The key to this is informing them of their rights in engagement letters or letters of employment.

We think it would also be sensible to consider the issuing of disengagement letters when clients move on and equivalent letters when staff move on.

You also need to make sure they know who the data controller is, why you need their data, where it will be dealt with and who will have access to it. If you intend to transfer their data to another country, you need to provide details of this and how and why the data will be protected.

6. Establish where your data is held and think about security

GDPR applies to all data, not just the electronically stored kind covered by the current rules. The rules are risk based, so you have to consider the risk of personal data being accessed by unauthorised people

Data held on paper, should not present much of a problem - filing cabinets with locks as appropriate and suitable archive facilities should, in the majority of cases, deal with the security issue, but you will have to make sure your systems are appropriate, depending on the sensitivity of the information stored.

Data stored, processed and transmitted electronically may present additional problems.

You need to know where the data is and what the security risks are, and you need to take steps to mitigate those risks.

- If it's held on site - can your systems be hacked?
- Does data leave the office on laptops, memory sticks or other devices?
- Where do you keep your backups?
- Is data transmitted by email or other electronic means?
- If you use the cloud, where are the servers? and do you need further permissions?

All of this should form the basis of your plan and, as we said at the beginning you need to have something in writing to show how you intend to proceed before 25 May.

Other sources of information

This article on AccountingWeb provides excellent sources of additional reading

Go Here

The guidance on ICAEW's website is also now pretty good:

Go Here

See our checklist on the next pages

...Strength in Numbers

The Society of Professional Accountants

5 St. John's Lane London EC1M 4BH
Tel: 0207 549 1698 | E-mail: mail@spa.org.uk

The SPA GDPR Checklist (1)

...Strength in Numbers

What sort of practice do you have?		
	Yes/No	**GDPR Implication**
Sole practice?		You are the data controller
>1 Principal through partnership/LLP/ Company?		Appoint a data controller
Personal clients?		Personal data held
Employees?		Personal data held, increased cyber risk
Sub-contract staff?		Personal data held, increased cyber risk
What sort of work does it do?		
Personal tax		Personal data held
Company secretarial		Personal data, processor rather than controller
Payroll		Personal data, processor rather than controller
Investment advice		Personal data held
Client money		Personal data, possibly processor rather than controller
Accounts		Will almost certainly involve some personal data
Audit		Audit files will almost certainly contain personal data, from payroll testing among other things
Probate		Personal data held

The SPA GDPR Checklist (2)

...Strength in Numbers

	Yes/No	GDPR Implication	
What IT and other systems do you have?			
Desktop			
Laptop			
Tablet			
Smartphone			
Internet connection			
Backup system			
Cloud (where are the servers?)		Potential security risk	
BYOD (bring your own device)		Potential security risk	
Memory sticks and external drives		Potential security risk	
Dropbox/Google drive?		Potential security risk	
Data protection and cyber			
Backup			
Firewall			
Malware protection			
How would you know if you'd been hacked?			

The SPA GDPR Checklist (3)

	Yes/No	GDPR Implication	
Transferring data			
Outsource?		Where is your outsource supplier located and are they GDPR compliant?	
Offshore?		Rules on transferring data to non EU member states	
Cloud?		Where are the servers?	
Transparency			
Employees - employment contract			
Clients - engagement letters			
Processor (rather than controller) engagement letter			
Other			