50 Osmaston Road
Derby DE1 2HU
Tel: 01332 345265

The Old Manse
29 St Mary Street Ilkeston
Derbyshire DE7 8AB
Tel: 0115 932 3995

3 Derby Road Ripley
Derbyshire DE5 3EA
Tel: 01773 743325

E-mail:
derby@mabeallen.co.uk
Website:
www.mabeallen.co.uk

Mabe Allen LLP
Chartered Accountants &
Business Advisers

J.P. Allen, FCA, FCCA, MABRP
K.C.G. Slack, FCA, FCCA
B. Sutton, FCA, CTA
C.J. Hopkinson, FCA, FCCA
D.J. Allen, BA (Hons), FCA, FCCA

Registered Auditors

Mabe Allen LLP is a
Limited Liability Partnership
registered in England and Wales.

Partnership Number
OC 308775

Registered Office
50 Osmaston Road,
Derby DE1 2HU

Registered to carry on audit work by the Institute of Chartered Accountants in England and Wales
Regulated for a range of investment business activities by the Association of Chartered Certified Accountants

NEWSLETTER

WINTER 2017

Changes to pensions auto-enrolment

The Pensions Regulator (TPR) reports that in the first part of 2017 alone, 136,000 small and micro employers began complying with their new responsibilities under the pensions auto-enrolment regime. That's an average of one every 57 seconds. But with change ahead, it's important to keep up to date with developments.

The latest important deadline is 1 October 2017, as the regime enters a new phase, with no lead-in time for new employers to comply. From 1 October, any employer taking on staff for the first time immediately comes within the rules. Those who have employed staff before 30 September 2017 have different deadlines – see the 'Duties Checker' section on the TPR site, **goo.gl/TXS6T5**

Ongoing duties

The first step in employer compliance involves assessing staff on the basis of age and earnings. Staff aged between 22 and State Pension age, who earn over £10,000 pa, (£833 per month or £192 weekly), must be put in a pension scheme, to which both employer and employee contribute.

But employer involvement doesn't stop there. If staff don't need to be put into a scheme, there's still a declaration of compliance to be made, and ongoing duties, including keeping track of employees' age and earnings each time they are paid, managing requests to leave or join a pensions scheme, and a three-year cycle involving re-enrolling employees who have opted out.

Next developments

The next major change to the regime is the increase in contribution rates from April 2018. From 6 April 2018 to 5 April 2019, employer minimum contribution increases to 2%, and from 6 April 2019 onwards, it rises again, to 3%.

Failure to comply can result in fines and being named and shamed on the TPR website. TPR is particularly vigilant regarding compliance: it has warned that it will prosecute for failure to provide information in the course of its investigations, and has initiated a first prosecution where an employer is held to have deliberately failed to put staff in a workplace pension.

Tax Goes Digital and Data Protection Regulations 2018

You will have read about HMRC postponing plans for quarterly online filing of accounting records. Whilst this gives us extra time, we are busy planning our resources to be able to assist all of our clients who are affected by this new initiative in 2019.

In addition, new Data Protection Regulations come into force in May 2018 which will affect every business regarding confidentiality of employees' and clients'/ customers' data.

Clearly we process a lot of confidential, personal data and we are therefore looking to improve our processes to ensure that we maintain the confidentiality and safety of your data.

We will shortly be contacting you with a new digital secure method of exchanging documents. This will enable us to send your tax return information and accounts to your personal, secure, digital letterbox called "Openspace".

We know that not every client will want this method of contact but believe that it will have many benefits in the way that we correspond with each other in the future.

Should you require further updates or advice on digital tax returns, please speak to your usual contact who will be pleased to advise you.

National Minimum Wage – where are we now?

Falling foul of the National Minimum Wage rules can be expensive – as well as having serious implications for employer reputation. Many firms have been named and shamed for getting it wrong - are you compliant?

Employer errors

The National Minimum Wage (NMW) keeps appearing in the headlines. Recently the Department for Business, Energy and Industrial Strategy (BEIS) announced that some 230 employers had been named and shamed for failing to pay NMW and National Living Wage (NLW). The retail, hairdressing and hospitality sectors were among the most non-compliant. Because of BEIS intervention, more than 13,000 low-paid employees were due to receive £2 million in back pay.

But the final price tag for employers who hadn't kept the rules was much higher. Between them, they were also fined a record £1.9 million. Business Minister Margot James said there was a clear message to employers. 'The government will come down hard on those who break the law.'

BEIS report that common employer errors include deducting money from employees to pay for uniforms, not accounting for overtime and wrongly paying apprentice rates to workers. So, what is the latest on NMW and how do employers keep on the right side of the law?

NMW and NLW – the basics

NMW is the least pay per hour most workers are entitled to by law. The rate is based on a worker's age and whether they are an apprentice. NLW applies to working people aged 25 and over. From 1 April 2017, the rate ranges from £7.50 per hour for those aged 25 and over, to £3.50 per hour for apprentices under 19, or for those aged 19 or over who are in the first year of an apprenticeship. Changes to NLW rates are in the pipeline from April 2018, so employers may need to plan for these now.

NMW/NLW rates are reviewed by the Low Pay Commission, but it is HMRC who police the system. Employers can be faced with court action if they don't pay NMW/NLW. Penalties for non-compliance stand at 200% of the back pay due to workers. The maximum penalty per worker is £20,000. There is a provision to reduce a penalty by half if unpaid wages and penalty are both paid within 14 days.

Not everyone qualifies for the NMW/NLW. These include people who are self-employed: volunteers: company directors: family members, or people who live with an employer and carry out household tasks eg au pairs.

But most other workers are entitled to NMW/NLW, including pieceworkers, home workers, agency workers, commission workers, part-time workers and casual workers. There are also rules regarding agricultural and horticultural workers, with slightly different small print for England, Scotland and Wales.

In calculating pay for minimum wage purposes, the starting point is total pay in a pay reference period - before deducting income tax and National Insurance. Some payments are not included, such as loans and pension payments.

To add to the complexity, there is also something called the Living Wage, which is an hourly pay rate, set independently by the Living Wage Foundation. This isn't anything to do with the government, and any employer who pays this does so entirely voluntarily.

Latest guidance: social care workers

HMRC have updated their guidance to clarify how NMW applies in the social care sector for workers carrying out 'sleepover shifts', following confusion over whether such shifts qualified for NMW. BEIS had suggested sleepover shifts carried out before 26 July 2017 qualified for a flat rate allowance, not NMW. But the decision is that NMW does apply, and applies retrospectively.

This could have left employers with bills of up to six years in back pay and penalties. But from 26 July, enforcement activity for sleepover shift pay is suspended until November, with retrospective penalties for sleepover shifts before 26 July 2017 waived. The actual back pay is still due, unless employers can show they can't pay. Although it is envisaged that underpayments will be pursued from this date, the government says it is committed to minimising the impact of future minimum wage enforcement in the social care sector.

When an employee is in crisis

Research suggests that one in ten employees is likely to be affected by bereavement at any given time. This can have many knock-on consequences in the workplace. Staff may need to take time off unexpectedly, find that their performance is affected, or be temporarily unable to carry out some roles. The law in this area is changing. What do you need to know?

Employment Rights Act

The Employment Rights Act is the law currently governing this area. It gives employees the right to take a 'reasonable' amount of *unpaid* time off in the event of an emergency involving a dependant. This includes making arrangements on the death of a dependant, and is likely to be agreed between employer and employee on an ad hoc basis. What is 'reasonable' in this context is not defined in the legislation, and the involvement of Acas or an employment tribunal would be a last resort here.

New legislation

The new, government sponsored, Parental Bereavement (Pay and Leave) Bill got its second reading in Parliament this autumn, and will change the law here. It will provide *paid* leave for bereaved parents for the very first time. The Bill's sponsor, Kevin Hollinrake MP, commented 'This is such an important Bill for parents going through the most terrible of times. There is little any of us can do to help, but at least we can make sure that every employer will give them time to grieve.'

In the meanwhile, employers can visit the Acas good practice guide for helpful guidance in this area. **goo.gl/aadWNQ**

Accidentally becoming a landlord

You may not think of yourself as a landlord - but do HMRC?

From time to time, HMRC run campaigns targeted at specific business sectors to help people bring their tax affairs up to date if they have inadvertently fallen outside the rules. At present, they are running a let property campaign, aimed at individual landlords letting out residential property abroad or in the UK, and recent guidance shows some of the ways that landlords can sometimes make mistakes **goo.gl/hTFbX5**

One of the most common mistakes is that people simply don't think of themselves as landlords. This can happen when someone inherits a property and then lets it out, or if they move in with a partner and then rent out their old house, or rent out a flat just to cover the mortgage payments. In fact, each of these scenarios means that HMRC need to be put in the picture, and the rental income could be liable to tax.

Other problem areas reported by HMRC are, for instance, property bought as an investment and rented out, and divorce situations where the matrimonial home is rented out and both partners move elsewhere. Difficulties are recorded where people relocate for work and rent out their house, or move into a care home and let out a house to help pay for care home fees. Issues can also arise with jointly-owned investment property, or when purchasing a property for a child at university, where other students also live there and pay rent on an informal basis. Members of the Armed Forces posted abroad, who let out a home in the UK, and people living in tied accommodation who let out a house, can also run into problems.

But it's not all bad news. One plus point for individuals (but not partnerships) letting out property on a small scale is the introduction of a new allowance – the property allowance – from 6 April 2017. There has been quite wide-scale coverage of this in the media earlier in the year. However, the allowance only gives relief for income of up to £1,000 in the tax year.

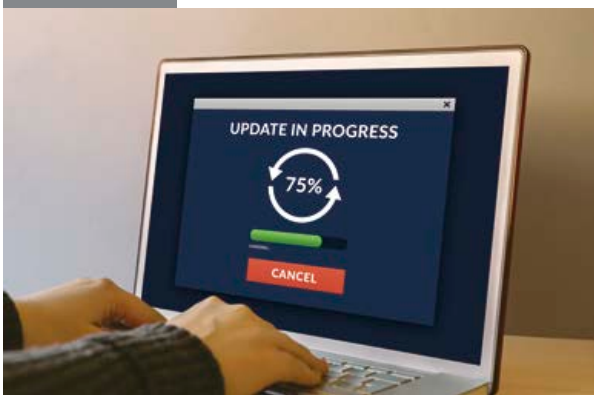
There can be unforeseen pitfalls – and tax planning possibilities - when letting out property. Please do talk to us if we can be of help in this area.

HMRC computer fix for personal tax returns

You may have heard that HMRC computer systems have had major problems correctly processing some 2016/17 self assessment tax returns. Essentially, there have been so many changes to personal tax legislation that HMRC software has struggled to cope.

One key problem area is the introduction of the Savings Allowance and the Dividend Allowance for the 2016/17 tax year. The main complication for HMRC was identifying and remedying scenarios in which it is not beneficial for a taxpayer to allocate personal allowances in the default order of 'non-savings income, then savings income, then dividend income'. In the new dividend tax regime there are a number of scenarios in which it may pay a taxpayer to reallocate part of the personal allowance to dividends - but HMRC systems were not always picking this up. The commercially provided software that we use as tax agents must follow HMRC specifications (even though some of the specifications may be incorrect), otherwise the returns filed online would be rejected.

Good news



The good news is that HMRC have now taken action to try to fix many of the problems, and amended the specifications for their 2016/17 tax calculator software. Such a late adjustment is unprecedented for HMRC, and the fix should be in place by the time you read this Newsletter. It should then be possible for those taxpayers affected to have their returns filed online as usual.

There will be some situations which will still not be resolved for the 2016/17 tax year but there will be an option for returns to be filed on paper even though the normal deadline for paper returns (31 October 2017) will have passed. We will be able to do this for you if necessary with a covering letter giving various technical details of what HMRC call the relevant 'exclusion' category. The extended deadline for such paper returns will be 31 January 2018. Should HMRC systems automatically generate a penalty for late filing, this will also be cancelled.

Please be assured that we are monitoring the situation closely. Should your affairs be affected, we will act to minimise your tax liabilities.

Making Tax Digital - plans for VAT

Earlier this year, the government announced that businesses operating above the VAT-registration threshold, (currently £85,000), would be the first to enter the new Making Tax Digital (MTD) regime.

Now there are indications as to what such businesses will have to do to comply, and when. The detailed rules should be in place by April 2018, with a view to a start date of 1 April 2019. Much work will be going on at HMRC and the software houses to get the scheme off to a smooth start.

Digital records

From 1 April 2019, businesses over the VAT threshold will be obliged to keep digital records and use MTD functional compatible software to give the information for their VAT returns to HMRC. They will have to preserve records in digital form for up to six years.

Software must be able to connect to HMRC via an Application Programming Interface, creating VAT returns and supplying HMRC with information digitally. HMRC are looking to harvest data on a voluntary basis as well, so they can monitor compliance, and also to provide information from their end. Business software would therefore need to be capable of accommodating this two-way information flow.

Supplying HMRC with quarterly information is one of the cornerstones of the MTD regime. But though VAT-registered businesses already supply quarterly VAT information, it isn't always an entirely digital operation. Many businesses use spreadsheets to submit returns, and HMRC may underestimate the change needed. HMRC state that the VAT account will link the underlying records and VAT return, but should a business use more than one software system, or spreadsheets, there could be complications. Add-on submission software will be needed for businesses using spreadsheets.

There are some exemptions from the requirement to keep digital records. These broadly follow those currently in place with regard to electronic VAT returns, covering members of religious societies, insolvent businesses, and those who 'for reasons of disability, age, remoteness of location, or any other reason' are not required to make an electronic return. A right of appeal is allowed if HMRC refuse exemption.

Businesses will have to keep and preserve what is called 'designatory data' digitally. This includes business name, principal place of business and VAT registration number, and information about any VAT scheme used: the VAT account, and information about supplies made and received.

Schemes and returns

HMRC say, 'The information contained with the VAT return will be generated by pulling information from the digital records. This information will contain as a minimum the nine boxes required for the VAT return, but can also contain a specific data set of supplementary information – all of which will be pulled from the digital records.' The procedure to correct errors will mostly be as at present.

Any business currently submitting monthly returns will continue to do so, as will any business submitting non standard returns. Users of the annual accounting scheme will be able to continue to do so. But the requirements for digital record keeping and submission will apply in these cases. Retail scheme users will be allowed to record electronically sales transaction data based on daily gross takings - rather than having to record details of each sale. For those using the Flat Rate Scheme, digital record keeping requirements will 'mirror' current record keeping requirements.

There will also be the facility for businesses to submit VAT information more often than the VAT return cycle requires, for example to keep HMRC informed of a change in circumstances. In the long run, HMRC are still looking to a scenario where income tax updates are made quarterly and digitally, and this is really what the VAT provisions anticipate.

Monitoring your VAT position

With VAT about to be linked to a new digital record keeping regime, it will be more important than ever to monitor business turnover to see if there is a need to register for VAT, as a business operating over the VAT threshold will enter a more complex regime. The requisite software is not yet available, but as we move towards MTD, many businesses may need guidance to make sure their systems are compliant, and we will be happy to advise on record keeping or in any other way we can.

https://online.hmrc.gov.uk/webchatprod/community/forums/list.page

HMRC

New HMRC online help for small business

HMRC have recently set up a new online forum and webchat facility to provide help for small businesses and the self employed. **goo.gl/rwJTBx**

It aims to provide guidance on starting in business, which legal structure to use, how to register and pay for taxes, and start-up finance, as well as helping with issues a growing business may face, such as expanding and taking on employees, buying and selling abroad, completing tax returns, working tax credit and child tax credit.

The forum aims to give general guidance, but is not able to provide answers to questions about individual circumstances. We can help with the specifics, so please do contact us where you need advice.

50 Osmaston Road
Derby DE1 2HU
Tel: 01332 345265

The Old Manse
29 St Mary Street Ilkeston
Derbyshire DE7 8AB
Tel: 0115 932 3995

3 Derby Road Ripley
Derbyshire DE5 3EA
Tel: 01773 743325

E-mail: derby@mabeallen.co.uk
Website: www.mabeallen.co.uk

Mabe Allen LLP
Chartered Accountants &
Business Advisers

J.P. Allen, FCA, FCCA, MABRP
K.C.G. Slack, FCA, FCCA
B. Sutton, FCA, CTA
C.J. Hopkinson, FCA, FCCA
D.J. Allen, BA (Hons), FCA, FCCA

Registered Auditors

Mabe Allen LLP is a Limited Liability Partnership registered in England and Wales.

Partnership Number: OC 308775

Registered Office: 50 Osmaston Road, Derby DE1 2HU

Registered to carry on audit work by the Institute of Chartered Accountants in England and Wales
Regulated for a range of investment business activities by the Association of Chartered Certified Accountants

Company secretarial duties update

The legal and administrative responsibilities involved in running a company are considerable, whether carried out by a company secretary, or another designated officer of the company. The advent of recent new legislation with regard to 'persons with significant control' adds further to the company secretarial burden. And as with other aspects of the company secretarial workload, there are significant penalties for getting it wrong.

This Briefing provides an up to date overview of the duties involved.

Do you need a secretary?

All public limited companies (plcs) are required by law to appoint a suitably experienced and qualified company secretary, but the position for private limited companies is different, and the secretary of a private limited company does not need specialist professional qualifications to act.

Since April 2008, private limited companies do not have to appoint a company secretary, unless this is an express requirement of their Articles of Association. In this case however, the work that would fall to a company secretary still forms an unavoidable part of a company's legal obligations.

If a company chooses not to appoint a company secretary, company secretarial duties will need to be carried out either by a director or by a person authorised by the directors. It is possible to delegate the work to professional advisers such as solicitors or accountants.

Key role

In 1993, a high-level report described the role of the company secretary in a plc like this:

'The company secretary has a key role to play in ensuring that board procedures are both followed and regularly reviewed. The chairman and the board will look to the company secretary for guidance on what their responsibilities are ... and … how these … should be discharged. All directors should have access to the advice and services of the company secretary and should recognise that the chairman is entitled to strong support from the company secretary in ensuring the effective functioning of the board.'

Although most relevant to plcs, there is a key message for all companies here: the work of a company secretary is vital.

As an officer of the company, the company secretary may be criminally liable for defaults of the company in some circumstances. This could be for example, failure to file changes in the details of the directors and secretary, or the company's annual return within the specified time limits. The responsibilities held by a company secretary should never be underestimated or undertaken lightly.

Duties

In return for the protection of limited liability, companies have historically been required to publish certain information in the public domain. This includes information relating to the accounts, details of the registered office, and details of directors and members, for example.

Providing and updating such information has usually fallen to the company secretary. The Companies Act 2006 does not specify the exact duties to be carried out by a company secretary, but they usually include the following:

- maintaining statutory registers (keeping company records up to date)
- completing and filing statutory forms (keeping the public record up to date)
- meetings and resolutions (making sure the company abides by both its internal regulations and the law).

Maintaining statutory registers

Companies are required to keep an up-to-date register of such details as:

- a register of members
- a register of directors
- a register of charges
- a register of persons with significant control.

It is important to note that the Companies legislation is backed up by a significant penalty regime. Failure to keep the registers up to date for example, can lead to a penalty of up to £5,000.

Persons with significant control

There have been recent important changes to the law in respect of the 'persons with significant control' (PSC) regime, particularly as regards reporting timescale and exemptions. A person with significant control is defined as an individual ultimately owning or controlling more than 25% of a company's shares or voting rights or who otherwise exercises control over a company or its management.

PSC changes to reporting timescale

Previously PSC information was updated annually, using confirmation statement CS01. Change is now event-driven, and must be reported to Companies House whenever it occurs. It can no longer wait until the end of the year. From now on, companies will need to use forms PSC01 to PSC09 to report these changes. When the annual confirmation statement is made, confirmation will be required that PSC information which Companies House already holds is accurate.

There are 14 days to update the PSC register and another 14 days to send the information to Companies House. That gives 28 days to notify Companies House of changes to the PSC register.

PSC exemption changes

Under the old rules, some companies were exempt from the PSC rules. These were DTR5 companies which are not on a regulated market. Under the new rules, such companies may have to comply. This could affect Alternative Investment Market companies (AIM) and ISDX (ICAP Securities and Derivatives Exchange) companies. If the company has traded on an EEA or Schedule 1 specified market, it is still exempt from providing PSC information. The Department of Business, Energy and Industrial Strategy has updated its guidance on the PSC register, and helpful guidance in this area can be found at **goo.gl/GZYtm1**

Completing and filing statutory forms

Company secretarial duties here include:

- Filing annual accounts at Companies House within the specified time limits. For a private limited company this is within 9 months of the accounting year end in normal circumstances
- Checking and confirming the annual confirmation statement issued by Companies House within 14 days - if necessary amending inaccuracies
- Notifying changes of directors, secretaries and their particulars to Companies House; changes in accounting reference date; changes in registered office; allotment of shares.

Please note that this list is not exhaustive. Many statutory forms can now be filed online via the Webfiling service at Companies House.

Meetings

Much company secretarial work involves the day to day administration of the company, for example ensuring that meetings of directors and shareholders comply with relevant legislation. The company secretarial role here would include issuing proper notice of meetings to those who are entitled to attend; preparing agendas; circulating relevant papers and taking minutes to record decisions taken.

Both members and auditors are entitled to notice of company meetings. At least 14 days' notice is required for a general meeting for a private limited company. Notice may be given in writing, or, in certain circumstances, online.

Private limited companies are no longer required to hold an Annual General Meeting (AGM) unless their Articles of Association expressly impose this obligation. A company which is required by its Articles of Association to hold an AGM may alter this by changing its Articles by special resolution.

Resolutions

A resolution is a legally binding decision made by the company. Resolutions may be of two types: ordinary resolutions and special resolutions. An ordinary resolution is one passed by a simple majority of members. A special resolution is one passed by a 75% majority of members.

Private companies can take most decisions by written resolution. This would not need hard copy and email may be used. It is important that the majority is correctly calculated however, being a majority of all members, and not just of those returning the voting papers.

Copies should be retained of important management decisions whether taken at a meeting or by written resolution. In some circumstances, these may need to be filed at Companies House.

Company name and registered office

There are very specific requirements relating to company name and registered office, and again it usually falls to the person exercising company secretarial duties to make sure the 'i's are dotted and the 't's crossed.

Every company (unless dormant since incorporation) must display a sign with its registered name at its registered office, any inspection place and any location at which it carries on business, unless this is primarily used for living accommodation.

The registered name must also be included in all business communications, both hard copy and electronic. The provisions here are quite specific. For instance, the signage must be in characters capable of being read with the naked eye, in such a way that visitors can see it easily, and displayed continuously. There is the proviso that if the location is shared by six or more companies, each company must display its registered name for at least 15 continuous seconds at least once in every three minutes. The high level of specificity here again serves as a reminder of the serious responsibilities involved in company secretarial duties.

The company registered name must be included in all forms of business correspondence and documentation, whether that be hard copy or electronic. Business letters; business emails; cheques signed by or on behalf of the company; orders for money, goods or services signed by or on behalf of the company, all fall into this category. Again the list is not exhaustive. The registered name must also be disclosed on company websites.

Further disclosure requirements

On all business letters, business emails, order forms and websites, a company must also state:

- the part of the United Kingdom in which the company is registered (i.e. England and Wales, or Wales, or Scotland, or Northern Ireland)
- the company's registered number
- the address of the company's registered office
- if a company is exempt from the requirement to use 'limited' in its name, the fact that it is a limited company
- if the company is a community interest company which is not a public company, the fact that it is a limited company
- if it is an investment company as defined by section 833 of the Companies Act 2006, the fact that it is this type of company
- if it is a company which has chosen to display its share capital, it must display the amount of paid up share capital.

How we can help

The legal and administrative burden placed on companies can seem very onerous indeed – especially for the small or medium sized enterprise. Should you wish to discuss company secretarial matters further, we should be more than happy to advise.

If for instance, you currently have a company secretary, and your Articles of Association permit, we can advise on the procedure to dispense with a secretary. We would also be able to undertake company secretarial duties on your behalf. Please do not hesitate to contact us if we can be of assistance in these areas.

50 Osmaston Road
Derby DE1 2HU
Tel: 01332 345265

The Old Manse
29 St Mary Street Ilkeston
Derbyshire DE7 8AB
Tel: 0115 932 3995

3 Derby Road Ripley
Derbyshire DE5 3EA
Tel: 01773 743325

E-mail: derby@mabeallen.co.uk
Website: www.mabeallen.co.uk

Mabe Allen LLP
Chartered Accountants &
Business Advisers

J.P. Allen, FCA, FCCA, MABRP
K.C.G. Slack, FCA, FCCA
B. Sutton, FCA, CTA
C.J. Hopkinson, FCA, FCCA
D.J. Allen, BA (Hons), FCA, FCCA

Registered Auditors

Mabe Allen LLP is a Limited Liability Partnership registered in England and Wales.

Partnership Number: OC 308775

Registered Office: 50 Osmaston Road, Derby DE1 2HU

Registered to carry on audit work by the Institute of Chartered Accountants in England and Wales
Regulated for a range of investment business activities by the Association of Chartered Certified Accountants

New data protection regime

Is your business prepared for forthcoming changes in the data protection regime? There has been extensive press coverage of the subject, but UK data protection watchdog, the Information Commissioner's Office (ICO), is now concerned about misinformation being circulated in the media.

With this in mind, we set out key features of the changes, with a view to dispelling some of the myths.

General Data Protection Regulation

From 25 May 2018, a new data protection regime comes into force in the UK. The General Data Protection Regulation (GDPR) will introduce key changes to the way personal data is handled. It stands regardless of Brexit, and the ICO advises businesses to plan now for compliance.

Why it's important

The new GDPR brings with it a new enforcement regime, which reflects the growing importance of safeguarding individuals' personal data in the digital age. At present, the maximum fine for breaches of data protection law is £500,000. Under GDPR, this rises to a maximum of £17 million or, if higher, 4% of worldwide annual turnover.

However, despite heavy media emphasis on penalties, the ICO insists that alternatives, such as 'warnings, reprimands, corrective orders', will always be considered. Of 17,300 data protection cases in 2016-17, only 16 resulted in fines. 'We have always preferred the carrot to the stick,' it says.

Negative publicity for failure to protect personal data is also a significant consideration. But there's a positive side, too. Good data protection practice offers a new means to create confidence and trust in the marketplace and workforce alike.

Areas of change

There are several important areas to consider. These are who and what is affected; controllers and processors; the principles of data protection; accountability and governance; new rights for data subjects; breaches of data security. We provide an overview of each of these in turn, below.

Who and what is affected

GDPR affects anyone handling personal data - from HR or customer records, to manual data, such as might be held in a filing cabinet, or electronic data accessed via a laptop, computer, or portable device.

The definition of 'personal data' is expanded under GDPR, and in addition, includes a range of 'online identifiers', such as IP addresses. Even pseudonymised personal data may be within scope, depending on how readily the data subject might be linked to the pseudonym used.

There is a further category to consider: 'sensitive' personal data. This comes under the heading of 'special categories of personal data' and a key change is that it now includes such categories as genetic data and biometric data which is processed to uniquely identify an individual. Whilst personal data relating to criminal convictions and offences is not included, there are extra new safeguards relating to how it is processed.

Controllers and processors

GDPR affects both controllers and processors of data. A controller is in charge of how and why personal data is being processed. A processor acts on behalf of a controller to process the data. It is possible for an organisation to act both as a data controller and a data processor, or it might fulfil only one of those roles.

Under GDPR controllers now have to make sure that any contract with a data processor is GDPR compliant. For the first time data processors are also within scope: they now have to keep records of how they process personal data, and can be held legally responsible for breaches of security.

Principles of data protection

The principles underlying GDPR are broadly similar to those of the current Data Protection Act (DPA). The requirements are that personal data must be:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary for the purpose
- accurate and kept up to date. Inaccurate data should be erased or corrected
- kept in an identifiable format for no longer than is necessary
- processed securely and protected from unauthorised or unlawful processing; accidental loss; destruction or damage.

However, there is now greater detail, and one major new addition to these principles. This keystone is the requirement for 'accountability.'

Accountability and governance

The new emphasis on accountability and governance means that you must demonstrate how your organisation is GDPR compliant. It is essentially about building data protection into organisational governance, from top to bottom.

Businesses must implement the necessary technical and organisational measures, including data protection policies (such as staff training; internal audits of processing activities; and reviewing HR policies). They must also keep a record of their processing activities, carry out data protection impact assessments where relevant; and appoint (in some circumstances) a data protection officer (DPO).

DPOs become a legal requirement in certain types of organisations, such as public authorities. Organisations carrying out particular types of processing, such as large scale monitoring of individuals, or large scale processing of special categories of data, or data relating to criminal convictions and offences, are also required to appoint a DPO.

The principle of data protection 'by design and default' is another key feature of GDPR. Some examples of appropriate measures suggested by the ICO include: data minimisation; pseudonymisation; transparency; allowing individuals to monitor processing; and creating and improving security features on an ongoing basis.

Organisations may also use approved codes of conduct and certification schemes to demonstrate compliance.

The ICO publishes much helpful information, including some key steps to getting prepared: **goo.gl/m2qPBE**

New rights

New rights for individuals have also been highlighted in the media. The issue of consent is one key area where much more rigorous procedures will be required under GDPR. Consent must be freely given, specific, informed, unambiguous, and methods such as pre-populated online tick-boxes will no longer be permissible. Existing consent procedures will need to be reviewed to ensure that they comply with the new rules.

Generally, GDPR sets out eight rights for the individual as follows:

The right to be informed

The right to know how personal data is processed. The GDPR promotes the idea of transparency in processing by means of a privacy notice, giving details of the controller; the source of the data; recipients of the data; data transfers made outside the EU; and the retention period of the data.

The right of access

Individuals may request details of information being held; how, why and where it is accessed; what categories of data are being accessed and who has access. The maximum time allowed to deal with such requests is reduced from 40 to 30 days. A subject access fee of £10, chargeable under the DPA, is removed under GDPR in most circumstances.

The right to rectification

The right to have inaccurate or incomplete personal data rectified, including personal data shared or given to third parties.

The right to erasure ('right to be forgotten')

The right to request deletion or removal of personal data where there is no compelling reason for its continued processing - including personal data shared or given to third parties. There are extra requirements when a request relates to a child, and some exceptions to this right, where data is held in order to comply with a legal obligation.

The right to restrict processing

Individuals may restrict the processing of personal data. Here personal data can be stored but not processed.

The right to data portability

The right to obtain and reuse personal data across different services, allowing movement, copying or transferring of personal data, and potentially enabling consumers to use applications and services to find a better deal. Personal data must be provided in a structured machine-readable format (such as .csv).

The right to object

The right to object to the processing of personal data. Processing must stop immediately unless there are 'compelling' legitimate grounds for processing, or processing is for the establishment, exercise or defence of legal claims.

Rights in relation to automated decision making and profiling

The right to ensure safeguards are in place to protect against the risk of damaging decisions being taken without human intervention. This extends to the safeguarding of personal data used for profiling purposes.

Breaches of data security

A data breach entails much more than simply losing personal data. It is defined as a security problem leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. ICO guidance gives the example of a hospital becoming responsible for a personal data breach where the health record of a patient is inappropriately accessed because of a lack of appropriate internal controls.

Media suggestions that every breach must be notified to the ICO are incorrect. Breaches must be notified when 'likely to result in a risk to the rights and freedoms of individuals' and notification must be made within 72 hours. But all organisations must plan to cope in the event of a security breach to demonstrate accountability due diligence.

How we can help

GDPR compliance cannot be achieved overnight. In this complex area, we are happy to provide further information or ongoing assistance.