Wright & Co Partnership Limited

Chartered Accountants and Registered Auditors

Issue 73

DECEMBER 2017

Wright in Touch

THE NEWSLETTER FROM WRIGHT & CO PARTNERSHIP LIMITED

WELCOME …

To the latest edition of Wright in Touch, our newsletter designed to bring you tax tips and news to keep you one step ahead.

Whilst the office is closed should you have concerns that need urgent attention please do not hesitate to contact us on the numbers shown below. Please note that an answer phone service is now available at both of our offices during closing hours, so if you would like to leave a message you will receive a call back the following working day.

We're here to help!

Contact us on:

Geoff – 07785 245669
Mike – 07831 489906

In this edition we have included information regarding the new Data Security – General Data Proection Regulation (GDPR). This will replace the existing Data Protection Act and will apply from 25th May 2018.

Published quarterly: *March, June, September and December.*

Abolition of Class 2 NICs delayed

On 2 November 2017, the Government announced a **one year delay to the abolition of Class 2 National Insurance Contributions** (NICs). Class 2 NICs will now be abolished from 6 April 2019 rather than 6 April 2018.

The delay will allow time for the government to engage with interested parties and Parliamentarians with concerns relating to the impact of the abolition of Class 2 NICs on self-employed individuals with low profits.

The relevant legislation will be contained in the National Insurance Contributions (NICs) Bill, which will now be introduced in 2018 with the measures it will implement taking effect one year later, from April 2019. These measures include the abolition of Class 2 NICs, reforms to the NICs treatment of termination payments and changes to the NICs treatment of sporting testimonials.

Broadly, Class 2 NICs are being removed to simplify the system. Those with profits below the small profits threshold (£6,025) will need to pay Class 3 contributions, which are five times as much as Class 2 contributions, if they wish to build up an entitlement to contributory benefits such as the state retirement pension. Based on 2017/18 rates, the proposed change would mean that people falling into this category would pay £592.80 a year more in Class 3 contributions.

According to the Office for National Statistics, there were 967,000 people with an annual income from self-employment below the small profits threshold in 2015/16. The proposals, as they currently stand, potentially impact on a considerable number of people.

Commenting on the delay, the Low Incomes Tax Reform Group (LITRG) said it was keen for a way to be found for the low-income self-employed to continue to be able to make affordable savings towards their pension at a rate similar to the present Class 2, perhaps by introducing a lower rate Class 3.

Childcare scheme extended

HMRC have recently confirmed that the second phase of the roll-out of the new 30 hours free childcare has commenced.

Broadly, from September 2017, the new 30 hours free childcare offer for working parents of three and four year olds in England doubled the previous 15 hours of free childcare, **saving eligible working families up to £5,000 a year**. From 24 November 2017, the service will also be available to parents whose youngest child is under six or who has their sixth birthday on that day.

Eligible parents will be able to apply online via the Childcare Choices website. On registering, they receive a code, which in turn allows them to arrange their childcare place. Parents can take their code to their provider or council, along with their National Insurance Number and child's date of birth. Their provider or council will check the code is authentic and allocate them a free childcare place.

Parents will be able to apply for tax-free childcare and the 30 hours offer in one go through the government's digital childcare service. Eligible parents can benefit from both tax-free childcare and 30 hours free childcare at the same time.

According to HMRC, more than 275,000 parents have already opened childcare account. Of these, more than 216,000 parents received an eligibility code for 30 hours free childcare for September.

Over the coming months, HMRC will gradually open the childcare service to parents of older children, while continuing to make further improvements to the system. The gradual rollout helps HMRC manage the volume of applications going through the service, so parents should continue to receive a better experience and prompt eligibility responses when they apply -HMRC claim that almost all parents receive a response within five working days, and most get their decision instantly.

All eligible parents will be able to apply by the end of March 2018.

HMRC consult on PAYE reporting requirements

HMRC have launched a technical consultation seeking comments on draft legislation which will amend the PAYE requirements (provided for in the PAYE Regulations) for employers in respect of car data reporting and optional remuneration arrangements. If enacted, the changes will apply from 6 April 2018.

Car data reporting requirements

Legislation was introduced at April 2016 that provided for employers to choose to tax most benefits-in-kind (BiKs) through their payroll rather than at the end of the year. These BiKs are reported to HMRC though Real Time Information (RTI), and remove the need for employers to submit forms P11D at the end of the year.

However, for company cars, **HMRC still need employers to provide data regarding the cars** and when draft legislation for voluntary payrolling was published for consultation in July 2015, HMRC advised that additional reporting requirements relating to car and car fuel benefit would be introduced for employers choosing to payroll car and car fuel benefit.

The changes to the PAYE Regulations being examined during the consultation period, set out what information employers will be required to report and how it will be submitted to HMRC.

Optional remuneration arrangements

Finance Act 2017 introduced legislation to remove the tax and employer NICs advantages of 'optional remuneration arrangements' (ORA) (commonly referred to as 'salary sacrifice arrangements'). Broadly, An ORA is where an employee gives up cash pay in return for a benefit-in-kind (BiK), which was usually taxed on an amount lower than the pay given up, or left untaxed. The new legislation specifies that now, where a BiK is provided in conjunction with salary sacrifice, the taxable amount will be the greater of the BiK calculated under normal rules or the amount of salary sacrificed.

As the amount of the calculation will be different under ORA, the changes to the PAYE Regulations will clarify the taxable amounts that need to be reported either via Real Time Information, where employers are payrolling BiKs, or at the end of the year for non-payrolling employers.

Further details can be found online at https://www.gov.uk/government/consultations/draft-legislation-the-income-tax-pay-as-you-earn-regulations-2017. Comments on the draft legislation are invited by 28 November 2017.

Employment status case turned on right of substitution

Employment status tax cases often make the headlines in the professional press and the recent case involving Deliveroo riders was no exception. The meal delivery firm won the case in the Central Arbitration Committee (CAC), confirming that its riders are not 'workers'. This is the latest challenge to the employment status of 'gig economy' workers.

In this case, the Independent Workers Union of Great Britain (IWGB) sought to argue that riders were workers, so that they could claim union recognition, thus affording them certain collective rights regarding the minimum wage entitlement, holiday and sick pay, and pension contributions.

The **CAC rejected the claim that the riders were 'workers'**, hinging the case on the riders' 'ability to turn down a job both before and after accepting it'.

Historically, a genuine right of substitution, whether 'sideways' to someone of similar seniority or by way of delegation to a junior, has been regarded as one of the strongest factors favoring self-employment.

The case follows a number of claims brought by workers in the 'gig' economy demanding rights such as holiday pay, the minimum wage and pensions contributions. Drivers at Uber won a recent victory when the company lost an appeal at the Employment Appeal Tribunal against an earlier decision to grant them workers' rights.

The transcript from the Deliveroo riders' case can be found at:
www.gov.uk/government/uploads/system/uploads/attachment_data/file/663126/Acceptance_Decision.pdf.

Data Security – General Data Protection Regulation

The General Data Protection Regulation (GDPR) will replace the existing Data Protection Act and will apply from 25th May 2018.

The new GDPR will require all organisations that deal with individuals living in a EU member state to protect the personal information belonging to those individuals and to have verified proof of such protection. Failure to comply with the new regulation will result in significant fines.

Whilst there are similarities between the Data Protection Act and the GDPR, there are some new and different requirements that all businesses need to be aware of, and act on, before May 2018. We hope this information will help you consider how to prepare for the implementation of the regulations.

SUMMARY OF NEW AND MODIFIED REQUIREMENTS

Here we summarise the new/modified requirements of the GDPR in comparison to the Data Protection Act.

There are perhaps a number of overriding principles and key words within the GDPR. These include transparency, accountability, consent, compliance and privacy by design. Some of the areas where these impact, include:

- **Controllers and processors** – there are some specific legal obligations for controllers and processors.
- **Controllers** – must specifically ensure that contracts with processors comply with the GDPR. Controllers shall also be responsible for, and be able to demonstrate, compliance with the GDPR data protection principles.
- **Processors** – are required to document records of personal data and processing activities, and are also legally responsible and liable for any security breaches.
- **Privacy notices** – The GDPR promotes transparency over processing by way of a privacy notice encompassing (amongst other things) 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.
- **Consent** – Consent must be freely given, specific, informed and unambiguous. Positive consent can no longer be inferred from silence, inactivity or the use of pre-ticked boxes.
- **Children's personal data and consent** – There are special provisions relating to the consent and processing of children's personal data.
- **Accountability and governance** – Organisations need to have 'comprehensive but proportionate' governance measures. For many organisations this is likely to mean more policies and procedures. And, for larger organisations (over 250 employees), this also means assigning or appointing a Data Protection Officer (DPO).
- **Subject Access Request (SAR)** – The time to respond to a SAR is now 30 days, and it must be provided free of charge unless the request is unfounded or excessive.
- **Notification of breaches** – breaches must be reported within 72 hours to the relevant supervisory/regulatory authority.
- **Data portability** – This is a new right under the GDPR, and allows an individual to request a machine readable copy of their personal data where processing is carried out by automated means.

SUMMARY OF KEY PREPARATORY STEPS

The ICO have produced a twelve step checklist to help organisations get themselves ready for compliance.

1. **Awareness** – the decision makers and key people in the organisation need to be made aware that law is changing. They need to appreciate the impact, and quantify and allocate resources to ensure compliance.
2. **Information held** – what personal data is held, where it came from and who it is shared with should be documented. It may be necessary to arrange for an information audit to be performed.
3. **Communicating privacy information** – existing privacy notices should be reviewed, and, if necessary, updated. Enhanced disclosure may be necessary to take into account all the new rights of individuals. If a privacy notice(s) does not exist, then one will need to be constructed.
4. **Individuals' rights** – review the eight key rights individuals have under the GDPR, and whether existing procedures and policies cover all these rights.
5. **Subject access requests** – update subject access rights procedures to take into account the rules.
6. **Lawful basis for processing personal data** – the lawful basis for processing activity should be documented and communicated in the privacy notice(s) – also see three above.
7. **Consent** – consent under the GDPR relies on a positive and transparent opt-in. Existing consent mechanisms and procedures may need to be updated.
8. **Children** – children's consent and children's personal data is given special protection under the GDPR. In some cases, a parent or guardian may be required to give consent.
9. **Breaches** – the right procedures need to be in place to detect, report and investigate a breach of personal data security. All organisations must report breaches to the ICO (as well as, perhaps, their own regulatory body).
10. **Privacy by design** – this is a legal requirement of the GDPR. In particular, an Impact Assessment should be performed even where it is not mandatory.
11. **Data Protection Officer** – someone in the organisation should be designated the responsibility for compliance. A Data Protection Officer is formally required in certain circumstances.
12. **International** – if the organisation operates in more than one EU member state, a lead data protection supervisory authority needs to be nominated. This is usually the country in which significant decisions are made about processing activities.

OTHER LAWS AND REGULATIONS

As well as the necessity to comply with the GDPR, there are various other Acts and regulations in the UK which have a bearing on data security. These include:

- Privacy and Electronic Communications Regulations (PECR) 2003 - which cover 'spam' and mass-marketing mail shots. Regulations under the PECR are also issued from time to time. For example, regulations on the use of cookies on websites, and in 2016 to require anyone making a marketing call to display their number.
- Copyright Design and Patents Act - amended in 2002 to cover software theft.
- There may be other IT standards and regulations applicable to your business sector: for example, companies processing credit card transactions need to ensure compliance with the Payment Card Industry Data Security Standards (PCI DSS).
- advising on appropriate procedures to ensure compliance with regulations applicable to the organisation and business sector.

Data Security – Data Loss Risk Reduction

Many companies are now completely reliant on the data stored on their network servers, PCs, laptops, mobile devices or in the cloud. Some of this data is likely to contain either personal information and/or confidential company information.

Here we look at some of the issues to consider when reviewing the security of your computer systems, and how to minimise the risks of data loss. We have a related factsheet which covers some additional considerations for those with data in the cloud, or use some form of outsourcing.

There have been many high profile incidents of data loss where large volumes of personal information have found their way into the public domain. Examples of this sort of information have included health records, financial records and employee details.

A commercial organisation also faces the additional risk of data being lost to a competitor.

Obviously, the larger data losses from government departments and corporations have hit the headlines. However, any company, no matter how large or small can suffer data loss unless sensible precautions are taken.

In the past year alone, according to recent research commissioned by the Department for Culture, Media and Sport (DCMS) some 45% of small/micro businesses have experienced some sort of security breach or cyber attack in the 12 months.

Over all sizes of business, the most common types of of breaches were - fraudulent emails (72% of all breaches), viruses and malware (33%), organisational impersonators (27%) and ransomware (17%).

AUDIT THE USE AND STORAGE OF PERSONAL DATA

Consider the potentially sensitive and confidential data which is stored by your business -

- staff records with date of birth, salary and bank account details, medical information etc
- customer and supplier records with bank/credit card account details, pin numbers, passwords, transaction information, discounts and pricing, contracts information
- financial and performance data and business plans.
- Confidential data is not always conveniently stored in a 'secure' database. Often employees need to create and circulate ad hoc reports (using spreadsheets and other documents) which are usually extracts of information stored in a database. This sort of data retrieval is quite often done at the expense of data security - as the database itself invariably will have access controls, but these ad hoc reports usually do not.
- Find out what is happening to data and what controls are in place to prevent accidental or deliberate loss of this information.

RISK ANALYSIS AND RISK REDUCTION

So the key question is - If all or some of this data is lost who could be harmed and in what way?

When that is known, then steps to mitigate the risks of data loss must be taken. Here are some steps which can be undertaken to reduce the risk of data loss -

- Undertake regular backups and store backup data securely off-site

- If high risk data is stored in the cloud understand what security mechanisms are in place and how you can retrieve all of this data if necessary
- Review the type of information which is stored on all devices (including laptops, mobiles, tablets etc) which are used off-site. If such information contains personal and/or confidential data try to minimise or anonymise the data. Ensure that the most appropriate levels of data security and data encryption are applied to this data
- If mobile devices are permitted to use company facilities ensure there is an active Bring your own Device (BYOD) policy in place, and appropriate security controls to restrict the type of data that can be stored on such devices
- Ensure that company websites which process online payments have the highest levels of security. This means adopting SSL encrypted transmissions.
- Review the use/availability of USB, and other writable media such as optical devices within the company and think about restricting access to these devices to authorised users only, via appropriate security settings, data encryption, and physical controls
- Ensure that company websites and networks are tested for vulnerabilities from attacks
- Have a procedure for dealing with sensitive information and its secure disposal once the data is no longer required
- Have a procedure by which any personal/corporate data stored on mobile devices can be wiped
- Train staff on their responsibilities, the data security procedures and what they should do if data goes missing
- Train staff to identify rogue emails, ransomware and malware, and other potential threats, and the procedures which should be followed.

SECURITY BREACH

As well as risk reduction, it is also good practice to have procedures in place in the event a security breach occurs. This should concentrate on four main areas -

1. A recovery plan and procedures to deal with damage limitation
2. Recovery review process to assess the potential adverse consequences for individuals, how serious or substantial these are and how likely they are, to happen again
3. Notification procedures – this includes not only notifying the individuals who have been, or potentially may be, affected. If the security breach involves loss of personal data then the Information Commissioner (ICO) should be informed. There may be other regulatory bodies and other third parties such as the police, the banks and the media who may need to be informed
4. Post-breach - ensure that appropriate measures are put in place to prevent a similar occurrence, and update procedures and train or re-train staff accordingly.

Data Security – Cloud and Outsourcing

Many companies are now completely reliant on the data stored on their network servers, PCs, laptops, mobile devices or in the cloud. Some of this data is likely to contain either personal information and/or confidential company information.

Here we look at some of the issues to consider when reviewing the security of your computer systems, and how to minimise the risks of data loss within the cloud and where some or all services are outsourced.

Whilst cloud data storage and outsourcing can often be more secure than using internal resources, there are some additional things to bear in mind when some, or all, of your data is not held on-site.

AUDIT USE AND STORAGE OF PERSONAL DATA

Consider the potentially sensitive and confidential data which is stored in the cloud by your business.

Find out what is happening to data and what controls are in place to prevent accidental or deliberate loss of this information.

RISK ANALYSIS AND RISK REDUCTION

So the key question is - If all or some of this data is lost who could be harmed and in what way?

When that is known, then steps to mitigate the risks of data loss must be taken. Here are some steps which can be undertaken to reduce the risk of data loss:-

- Ensure that the cloud provider or outsourcer will not share your data with a third party
- Check in what countries the data will be stored and processed – as this could have Data Protection implications
- Ensure that you can take local backup copies of your data
- A data subject has the same rights of access wherever data is being stored, so ensure that a subject access request can be facilitated
- Try to minimize the amount of personal data stored in the cloud or with a third party
- What happens if the provider becomes insolvent? Have a contingency plan in place
- Is the data encrypted – if so have you got access to the keys and who else has access to the keys?

There are many resources available, but we have included two examples here:-

https://www.cesg.gov.uk/cloud-security-collection

https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

Data Security - Backup

Many companies are now completely reliant on the data stored on their network servers, PCs, laptops, mobile devices and in the cloud. Some of this data is likely to contain either personal information and/or confidential company information.

Here we look at some of the issues to consider when reviewing the security of your computer systems and data.

Data backup is an essential security procedure and needs to be undertaken on a regular basis. A business should view regular backups as a form of insurance policy.

There are a number of points to consider.

SYSTEMS AND APPLICATIONS SOFTWARE INSTALLATION MEDIA

Ideally, once software has been installed, the original media (unless the software was downloaded) should be stored securely off-site. Any activation keys/codes should be similarly stored securely.

DATA FILE LOCATIONS

In a network environment some data files might be stored on the server and other data files stored on local drives. In which case, separate backups may be required for both the server and one or more PCs.

Ideally, a network solution should be provided which ensures that all data is re-copied back to the server from local drives.

BACKUP STRATEGY AND FREQUENCY

There is likely to be a need for two parallel backup procedures; one to cover a complete systems backup of the server(s) and another to incrementally (or differentially) backup data files which have been updated since the previous backup.

The most common backup cycle is the grandfather, father, son method. With this, there is a cycle of 4 daily backups, 4/5 weekly backups and 12 monthly backups.

Remember that some data has to be preserved for many years - for example accounting records need to be kept for a minimum of 6 years.

Backup media can be re-used many times, but they do not have an infinite life and will need replacing after 2-10 years depending on quality and number of times used. Some additional points are made on this issue in the section on backup media degradation.

BACKUP RESPONSIBILITIES

Someone should be given responsibility for the backup procedures. This person needs to be able to:

- regularly ensure that all data files (server and local) are incorporated in the backup cycle(s)
- adapt the backup criteria as new applications and data files are added
- modify the backup schedule as required
- interpret backup logs and react to any errors notified
- restore data if files are accidentally deleted or become corrupt
- regularly test that data can be restored from backup media
- maintain a regular log of backups and where the backup media are stored.

APPLICATIONS BACKUP ROUTINES

Many accounting and payroll applications have their own backup routines. It is a good idea to use these on a regular basis (as well as conventional server backups) and always just before critical update routines. These backup data files should be stored on the server drive so that they are backed up.

LOCAL PCS

Certain users will have applications data files exclusively on their local drives (such as payroll data for example) and these will require their own regular backup regime, which as mentioned in the previous paragraph, may consist of a combination of backing up to media and backing up to the server.

BACKUP MEDIA

Selecting the right media to use for backups depends on budget, how much data there is and the networking operating software. External hard disks or a NAS box with cloud backup may provide a good solution. If an external service provider is used, or perhaps a cloud option, they should have their own backup regime – but don't totally rely on this.

Optical storage such as CD/DVD, or Blu-Ray may also be considered as a cheaper alternative, but capacity and life may be limited.

BACKUP LOCATION

Backups should be stored in a variety of both on-site and off-site locations. On-site backups are easily accessible when data has to be restored quickly, but are at risk from either fire or other disaster.

A large number of businesses use an on-site safe, however, in a recovery situation this could be buried under tons of rubble, or the premises themselves may be inaccessible for a period of time.

Off-site backups have the advantage that they can be recovered in an emergency, but

a) they still need to be stored securely; and

b) need to be reasonably accessible.

BACKUP RETENTION

Finally, certain type of records, such as accounting records for example, need to be kept for a minimum period of time and this must be considered when developing the data backup strategy (also see below regarding degradation).

BACKUP MEDIA DEGRADATION/DECOMPOSITION

Backup media degrades and the data stored on them decomposes over a period of time.

Optical media such as CD/DVD and Blu-Ray are particularly sensitive to light (photosensitive), so ensure that they are stored in a dark environment. They are also prone to physical damage when being handled. Finally, this type of media is not designed for long-term storage - lasting possibly as little as 2 years.

Backups should be checked on a regular basis for signs of digital decomposition, and tested to check that data can be successfully restored.

IN-HOUSE OR CLOUD?

Many internet service providers and third-party IT service organisations, now offer, either as standard or as a chargeable extra, off-site data repositories and also complete online application solutions. The immediate appeal is that there is no need to internally support a server and its operating and applications software. However, there are a significant number of key security issues which should be covered as part of the contract/service level agreement (SLA). These should include level of encryption, the countries in which the data is processed and stored (as this has potential issues with Data Protection laws), data deletion and retention periods, the availability of audit trails of who is accessing the data and finally, who has ownership of the data if the provider goes into administration/receivership.

Where data is stored in the cloud, try to ensure that as little personal data as possible is processed and stored in this way. If this is not possible then at least anonymise the data so that individuals cannot be identified.

Ensure you can manually take your own backup copies of data stored with a third-party, and that this data is in a readable format and can be restored onto other services and applications.

Data Security – Access

Many businesses are now completely reliant on the data stored on their Network Servers, PCs, laptops, mobile devices and cloud service providers or internet service providers. Some of this data is likely to contain either personal information and/or confidential company information.

Here we look at some of the issues to consider when reviewing the security of your computer systems with respect to access controls, and to ensure compliance with Principle 7 of the Data Protection Act. This states that -

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

ACCESS SECURITY

Good access controls to the computers and the network minimise the risks of data theft or misuse.

Access controls can be divided into two main areas:

- Physical access - controls over who can enter the premises and who can access personal data
- Logical access - controls to ensure employees only have access to the appropriate software, data and devices necessary to perform their particular role.

PHYSICAL ACCESS

As well as having physical access controls such as locks, alarms, security lighting and CCTV there are other considerations, such as how access to the premises is controlled.

Visitors should not be allowed to roam unless under strict supervision.

Ensure that computer screens are not visible from the outside.

Use network policies to ensure that workstations and/or mobile devices are locked when they are unattended or not being used.

Ensure that if a mobile device is lost it can be immobilised remotely.

Mobile devices being small are high risk items so sensitive data should always be encrypted and access to the service should be controlled via a pin number or password.

It may be necessary to disable or restrict access to USB devices and Optical readers and writers.

Finally, information on hard-copy should be disposed of securely.

LOGICAL ACCESS

Logical access techniques should be employed to ensure that personnel do not have more access than is necessary for them to perform their role.

Sensitive data should be encrypted and access to this data controlled via network security and user profiles.

Access to certain applications and certain folders may also need to be restricted on a user by user basis.

Finally, it may be necessary to lock down certain devices on certain machines.

PASSWORDS

A password policy consisting of a username and password is good practice.

These help identify a user on the network and enable the appropriate permissions to be assigned.

For passwords to be effective, however, they should:

- be relatively long (i.e. 8 characters or more)
- contain a mixture of alpha, numeric and other characters (such as &^")
- be changed regularly through automatic password renewal options
- be removed or changed when an employee leaves
- be used on individual files such as spreadsheets or word processed documents which contain personal information

and should NOT

- be a blanket password (i.e. the same for all applications or for all users)
- be written on ‘post it’ notes that are stuck on the keyboard or screen
- consist of common words or phrases, or the company name.

FESTIVE CLOSING DATES

As 2017 draws to a close, we'd like to take this opportunity to thank all of our valued clients for their support throughout the year and wish everyone a safe and happy Christmas and New Year.

Wright & Co Partnership Limited will be closed from 10.30am on Friday 22nd December 2017 reopening on Tuesday 2nd January 2018 at 8.30am

For any urgent enquiries over this close-down period please email info@wright-co.com
or contact Geoff on 07785 245669 or Mike on 07831 489906

We look forward to working with you in the New Year!

Question and Answer Section

My wife and I jointly owned a property that we originally lived in for many years, although it has been rented out for the last 10 years. My wife has recently died and I am now the sole owener of that property. I intend to sell it and give the proceeds to my two children (both aged in their 40's). Will there be a capital gains tax on the sale proceeds?

If a residence is transferred between a husband and wife who are living together (or between civil partners), of each other who are living together, whether by sale or by gift, the period of ownership of the transferee is treated as beginning at the beginning of the period of ownership of the transferor (TCGA 1992, s 222(7)(a). This also applies where the residence is transferred from one to the other on death. When you inherited your wife's half share in the property, you also took over her principal private residence 'history' for that property. This means that if you sell the property now, you will be entitled to PPR relief for all the period you occupied the property plus relief for the final eighteen months of ownership.

Additionally, you should be able to claim the letting exemption to reduce the gain attributable to the ten years that you rented it out.

I have not yet paid my self-assessment payment on account, which was due on 31st July 2017. Will I be charged a penalty for paying late?

Interest will be charged on the overdue amount. The charges will accrue from the due date of payment (31st July 2017) to date the payment is made. The applicable interest rate is currently 2.75%.

Penalties, on the other hand, will only be imposed if the balancing payment (due 31st January 2018) is late. The penalties for late payment under self-assessment are as follows:-

- 30 days late: 5% of the unpaid tax
- 6 months late: additional 5% of the unpaid tax
- 12 months late: additional 5% of the unpaid tax.

HM Revenue & Customs may reduce a late payment penalty in 'special circumstances', which does not include inability to pay. In addition, a defence of 'reasonable excuse' may be available.

In relation to payments on account, the maximum penalty for fraudulent or negligent claims by taxpayers to reduce payments on account is the difference between the correct amount payable on account and the amount of any payment on account made.

Directors: Mike Atkinson & Geoff Whiting

Contact Us

Wright & Co Partnership Limited
The Squires, 5 Walsall Street, Wednesbury
WS10 9BZ
Tel: 0121 556 1072
Fax: 0121 505 1557

9 Stafford Street, Brewood,
Stafford, Staffordshire ST19 9DX
Tel: 01902 850828
Fax: 01902 850331

info@wright-co.com
www.wright-co.com

NEED HELP ?

Please contact us if we can help you with these or any other tax or accounts matters.

In addition, if there's anyone else who you think would benefit from the newsletter, please forward the email to them or ask them to contact us to be added to the newsletter list.

ABOUT US

WRIGHT & CO PARTNERSHIP LIMITED has been established for over 50 years, and is a modern and progressive accountancy firm, committed to offering a high quality service to an ever expanding and varied client base.

Two directors assisted by a skilled team of fourteen offer a wide range of experience in all aspects of the profession.

Over the years we have expanded and developed a range of services to meet the needs of the vast majority of businesses, from the smallest sole-trader to limited companies with turnover of several million pounds.

OUR SERVICES

Audit and Accounts

Charities audit

Academy schools audit

VAT

Construction Industry Contracts fo Service

Payroll, Real Time Information & Pension Auto Enrollment

Book-keeping

Sage training

Business and Tax Planning

General Business Services

Corporate Services

Taxation Services

Business Start-Ups

Making Tax Digital

Solicitors Accounts Rules

Trust and Estate Advice

Company formations

Company secretarial