MOORE Kingston Smith

ASSOCIATION MATTERS

In this issue:

WELCOME TO OUR LATEST TRADE ASSOCIATION AND MEMBERSHIP BODY NEWSLETTER

It has been a year since Coronavirus took over our lives and even though some form of lockdown is still on the horizon, there is light at the end of the tunnel with the rollout of the vaccination in full swing.

Our number one priority has always been to support you and your organisation through our many webinars and e-bulletins. Our Coronavirus hub has all the latest news and I hope that you have had a chance to read our updates.

In our latest edition of Association Matters we highlight three topical areas which your organisation should already be looking at.

Our first article is a reminder of the new off-payroll working rules which were due to come into effect in April last year, but were postponed due to the pandemic. Now due to be implemented on 6 April 2021, we look at what the changes mean for your organisation – especially if you use consultants.

With more people than ever working from home, this has caused major concerns over cyber security. With security breaches hitting record levels, our next article looks at cyber security and the pitfalls to watch out for. We also look at the steps you can take to protect your organisation.

On page six of this newsletter you will find details of the cyber security webinar we are holding on 18 March. I hope you can join us.

In our final article we focus on wellbeing, an area that is increasingly important as we emerge from lockdown. Our HR consultancy team provide their top 10 tips on how you can support your employees' wellbeing.

We hope you find this edition of Association Matters helpful. If you would like to discuss any of the articles in more detail, please get in touch.

Janice Riches
Head of Trade Associations & Membership Bodies
jriches@mks.co.uk

NEW OFF-PAYROLL WORKING RULES FOR CONTRACTORS AND CONSULTANTS

By John Williams, Senior Tax Manager,
Moore Kingston Smith

Membership Organisations should be preparing now

The new off-payroll working rules (also referred to as IR35) in the Finance Act 2020 come into effect on 6 April 2021. For organisations relying on a consultant workforce, or using contractors to create a more flexible workforce to boost their recovery from the business effects of Coronavirus, it is now more important than ever that you prepare for the off-payroll working rules ahead of April.

The Finance Act 2020 widened the circumstances in which a contractor providing their services via a limited company to an organisation could be subject to the new off-payroll working rules. The Finance Act also included some additional detail to the various processes, including issuing status determination notices and dispute resolution procedures.

What do the changes mean for your organisation?

The new rules will mean that when your organisation is engaging with individuals, consultants, contractors or freelancers who provide their services through their own company (common place for IT, Marketing and some Finance services), your organisation will be responsible for deciding if tax should be deducted at source (e.g. PAYE). So, if you determine the individual is regarded as an employee and is providing their services directly to your organisation, you will need to deduct income tax and employee NICs and pay employer NICs even when the services are provided through a personal service company.

If your organisation is paying an agency that has the contract with the individual's personal service company, the agency is responsible for deducting these payroll taxes. However, you, as the end user of the services, must tell the agency, as well as the contractor, whether the off-payroll working rules apply.

Will these rules apply to all organisations?

These new off-payroll worker rules will apply to medium and large organisations. An exemption from these rules is currently available for small organisations.

The main tests for determining whether an organisation is small are taken from the Companies Act 2006. To be treated as small, two of three conditions need to be satisfied:

- Annual turnover of not more than £10.2 million
- Balance sheet total of not more than £5.1 million
- Number of employees not more than 50.

Even if you are a small organisation at the moment and currently exempt from the off-payroll worker rules, this could change going forward. HMRC has continually expanded the application of the off-payroll rules and may well expand them to apply to small organisations in the future. To be ready for this possibility, many small organisations are assessing arrangements with potential new contractors to ensure they are treated correctly from the outset.

If you need help in reviewing individual contractor arrangements, want to ensure arrangements with potential new contractors are set up correctly or you are on the borderline of not being a small company, please contact us.

Some common areas of misunderstanding

- Just because your consultant advises your organisation that they consider themselves as self-employed does not mean they are - it is your organisation's responsibility to determine whether the indicators for self-employment are met.
- All payments to directors for their services as an office holder (including non-executive directors) of a company must be processed through the payroll with PAYE and National Insurance accounted for. This applies to all fees/remuneration/honoraria/benefits earned as an office holder.

Key risks for your organisation

- Substantial increase to your compliance burden putting strain on your organisation's existing resource.
- Getting the determination wrong. The approach taken in HMRC's Check Employment Status for Tax tool does not currently accurately reflect the full range of case law on employment status and has faced much criticism.
- Where failure of obligations under these rules arise anywhere in the supply chain, HMRC could potentially seek payment for tax and NIC from your organisation even where you are not responsible for deducting PAYE and NIC.
- The cost to your organisation of using a contractor where the off-payroll working legislation applies has increased by up to 14.3% (current employer's NIC charge and apprenticeship levy).

How Moore Kingston Smith can help you

Moore Kingston Smith offers an off-payroll working solution to suit your needs. By drawing on our experience with the existing public sector regime (in force since 2017), we can advise trade associations and membership organisations on the off-payroll working rules legislation, HMRC guidance, and how to deal with HMRC on general employment status issues.

We can help you by:

1. Assessing the workforce to identify the consultants who fall under these new rules and perform status determinations from a review of existing contracts.
2. Advising on your communication strategy with the individuals in the time leading up to 5 April 2021 and beyond to warn them of these changes.
3. Providing guidance on issuing Status Determination Statements.
4. Reviewing your processes and systems to ensure that contracts for personal services are identified and handled correctly. This will include determining their status and passing on the correct notices, as well as providing the correct sums to payroll for calculations on the necessary deductions.
5. Providing guidance on the dispute resolution process and creation of a policy to comply with your statutory obligation.

CHALLENGING COMPLACENCY: ARE YOUR E-COMMERCE SERVICES AT RISK OF A CYBER ATTACK?

By Maritz Cloete, Director of Cyber Security, ClearComm

The Government's Cyber Security Breaches Survey 2020 indicates that cyber attacks have evolved and become more frequent. Almost half of businesses surveyed reported breaches or attacks in the 12 months prior to the survey, with 32% of affected businesses claiming at least one incident per week.

Trade associations and membership bodies may be tempted to breathe a sigh of relief at learning that only 19% of affected businesses lost money and/or data as a direct result of an attack. However, attacks don't have to be successful to be disruptive. Twice as many of the affected businesses (39%) claimed that they had experienced a negative impact as a result. This included having staff time diverted, needing to put new measures into place or wider business disruption.

Cyber criminals are targeting online trading

Online retailers certainly benefited from the COVID effect. Online sales rocket by 33% last June, even as some major retailers emerged from lockdown with renewed online business strategies. At Christmas, even seasoned Christmas shoppers preferred to tackle their shopping online rather than donning masks to face the socially distanced queues on the high street.

Of course, where there are opportunities for online trading there are also opportunities for cyber criminals, with web store vulnerabilities ripe for exploitation. One of the cyber criminal's favourite weapons of choice involves compromising e-commerce websites or service providers and planting skimmer malware which harvests customers' personal and financial information. Such 'Magecart-style attacks', named after the Magecart consortium of hacker groups, have been phenomenally successful, netting attackers more than £5 million from over 550 website hits in the last three years alone.

As well as skimming card details, cyber criminals also fraudulently purchase goods, redirect customers to malicious websites and abuse web servers to host malicious content.

The cost of inaction

If you do trade online, preventing your e-commerce site from being breached is one of the best ways to protect your income. The costs of preventing a breach are far less than the costs of putting a breach right – as far as it can be put right. Those who fail to secure their online premises face a raft of costs including:

- Forensic investigation costs – mandatory costs which can run into many thousands of pounds (especially if credit card data is stolen).
- The cost of notifying member customers as required by the GDPR and UK DPA.
- The cost of reparations for member customers, such as paying for credit monitoring services for affected consumers.
- Fines, for example from their payment processors or the ICO.
- To these they can add intangible costs, such as loss of trust. Reputational damage can result in reduced members' lifetime spend, decreased membership retention, a decrease in recommendations, lost market share and damaging reviews or comments on social media.

Protecting your online trade

Online activity is not entirely at the mercy of cyber criminals. You can protect your online trading estate and your members' data by considering the following key steps:

- Demonstrate the authenticity of your website through the use of website certificates (also known as SSL certificates). Always use HTTPs with a certificate from a trusted certification authority to protect customer interactions with your website.

- Ensure that your web servers, web e-commerce applications and any plug-in software is configured in line with best practice and patched as regularly as possible, even daily if practical. Cyber criminals maintain inventories of e-commerce sites and the versions of software deployed so they can quickly attack vulnerable sites when new security patches are announced.
- Make sure any website administrative functions, such as site configuration panels, are adequately secured and that access is highly restricted. Consider using multi-factor authentication for all site administration activities to reduce your exposure to password guessing and password spraying attacks.
- Closely monitor changes to your website content at a server file system level, as unauthorised changes may be an indication that your site may have been compromised by a cyber criminal.
- Backup your website regularly so that you can recover to a known secure position if you are compromised.
- Regularly commission security experts to carry out web application security tests to confirm your e-commerce site does not have any exploitable vulnerabilities. Do this every time you make major changes to your e-commerce site, or at least annually if your site is not subject to any major upgrades or changes.

Strengthen your frontline defences

After a recent high-profile hack, Twitter said that hackers had targeted employees "with access to internal systems and tools." A BBC article claims that "the consensus in the information security community is that Twitter's employees were likely duped by a spear-phishing attack via a phone call. This involves using friendly persuasion and trickery to get victims to hand over crucial information that enables hackers to infiltrate a company's systems."

Now, with your employees' attention at least partially diverted away from their day-to-day jobs, your vulnerabilities are higher than ever. Luckily, there are several steps you can take to minimise risks:

- Ensure all users – regardless of age or position complete online cyber security training, such as that provided by the National Cyber Security Centre.
- Warn users about new phishing scams.
- Circulate news stories about businesses affected by cyber crime.
- Regularly remind them to remain alert, especially when receiving unexpected messages by email, instant messaging apps, text and conference call apps.
- Discourage them from clicking on links in messages or opening attachments without first verifying that they are legitimate and safe.
- Make sure users with privileged access to your systems - such as developers and tech support staff - take particularly good care of their login credentials and receive the training necessary to allow them to manage your website security effectively.

We also recommend that you ask employees to forward any suspicious emails to report@phishing.gov.uk for investigation.

Consider certification

Cyber Essentials Plus and/or ISO 27001, the Information Security Management Standard won't just protect your business. These certifications can differentiate you from your competition and reassure potential members and donors.

In summary

Every business is at risk from cyber crime. Criminals are constantly on the lookout for loopholes to exploit, regardless of size, location or sector.

Trade associations and other membership bodies need to increase their cyber security resilience to protect their services, data and reputation. Failure to do so could be catastrophic.

ClearComm is part of Moore Kingston Smith, a dynamic led professional UK firm of accountants and business advisers delivering Data Privacy, Cyber Security, Business Continuity and Information Security solutions to organisations worldwide.

SUPPORTING EMPLOYEE WELLBEING DURING AND POST-PANDEMIC

By Holly Bateson, HR Consultant, Moore Kingston Smith HR Consultancy

The CIPD disclosed in their 2020 '*Embedding new ways of working – Implications for the post-pandemic workplace*' report that 47% of employers have cited reduced mental wellbeing amongst employees as their biggest people challenge throughout the pandemic. Whether your employees have been furloughed, are working from home, shielding or have suffered from COVID-19 over the past year, each individual will require personalised support returning to work and maintaining their physical, mental, social and financial wellbeing.

The unprecedented disruption for such a long period of time has subsequently resulted in an increase of worry and stress for employees in all sectors. CIPD's report has found that employees are significantly worried about their health and that of their family, the impact of isolation and loneliness on their wellbeing, the risk of being made redundant and their overall finances.

Moore Kingston Smith HR Consultancy have pulled together their top 10 tips on how trade associations and membership bodies can support their employees' wellbeing now and in the future.

1. Establish robust communication channels with employees to understand their concerns and help avoid a one-size-fits-all approach. Individual one-to-ones with line managers provide a platform for employees to voice concerns and the opportunity to create a wellness action plan to support needs. Group meetings can also be efficient but not all employees will feel comfortable opening up in this environment.
2. Encourage employees to check on their fellow colleagues regularly throughout this difficult period of time. Allow time for employees to have more social breaks throughout the day to provide essential interaction for those who have been, or still are, isolating alone.
3. Be transparent about what you do and don't know to help build trust in a very difficult time. Share your priorities for the organisation and decisions in an efficient and transparent way to help reduce employee anxiety. Employees want security but being direct about any changes to the structure, their remuneration or benefits straight away can allow employees to plan for the future.
4. Provide access to an Employee Assistance Programme (EAP) or invest in trained Mental Health First Aiders and make it easy for employees to reach out for confidential counselling and support. Don't forget that the EAP line can be a great source of support for managers who need guidance if they are worried about an employee's wellbeing.
5. Encourage employees to eat healthily, keep active and to be mindful of their alcohol intake to proactively promote positive physical and mental wellbeing. Whether you are able to get together physically or virtually, organising activities that don't always revolve around alcohol or baked treats can promote a healthy balance and can often be more inclusive.
6. If a group of employees experience a traumatic event together, offer critical incident stress management workshops to help everyone process what they have been through via activities and group discussions.
7. Reaffirm when you expect employees to be contactable, ways of working remotely and regularly checking in to discuss their workload to help encourage a positive work/life balance. Some employees working from home have expressed that it is hard to switch off and have reported doing longer hours. It is also important that senior leaders role model these behaviours and set reasonable deadlines.
8. Issue remote working and wellbeing policies to help clearly communicate expectations and give employees a sense of ownership and boundaries. Although implementing policies can feel quite corporate and formal, they are also ways for employees to find the details of any support they require independently.
9. Hold appraisal meetings and set reasonable objectives in light of the pandemic to help keep employees motivated and know what they are working towards. With so much change it is inevitable that plans and objectives at the start of the year will need to be reassessed.
10. Create a physical or virtual wellbeing hub that is regularly updated so that employees can easily find the support they need. This allows employees to review resources at their own convenience and can be a great tool for line managers to help their employees find the right support.

Consistently supporting employee wellbeing will help individuals as they come to terms with the impact of the pandemic. Employees who have experienced severe financial hardship or those that are grieving the loss of close family and friends through ill health, may require further support. Returning to 'normal' will not be easy, but approaching every decision and update with employee wellbeing in mind, will have a positive impact for all.

References

CIPD. (2020) *Embedding new ways of working: implications for the post-pandemic workplace* London: Chartered Institute of Personnel and Development.

If you are interested in any of the articles published in this newsletter, please contact us at pd@mks.co.uk, quoting Association Matters March 2021.

WEBINAR: RANSOMWARE 2.0 – CYBER CRIMINALS RAISE THE STAKES AGAIN

The volume and impact of cyber attacks on UK organisations remain alarmingly high, and in particular, many small and medium-sized companies are still falling victim to ransomware, with disastrous effects on their organisation. For trade associations and membership bodies who hold a vast amount of member data, they have to be particularly vigilant.

With both the ease with which ransomware malware can be 'rented' and profit-sharing arrangements between the criminal and the malware authors, ransomware continues to be a very lucrative revenue stream for criminals. Attackers are also employing 'double-extortion' techniques by first stealing and then encrypting a victim's data, and then extorting the victim for a decryption key as well as a guarantee that the stolen data will not be made public. With the threat of major financial penalties under the UK DPA and GDPR, many victims feel they have no choice left but to pay the ransom, as the alternative may be business closure.

In this webinar, we will show you, through a live hacking demonstration, some of the most common ways a cyber attacker could infect your organisation with ransomware. We will also talk through what you can do as a business to protect yourselves against this rise in cyber criminality, and to avoid becoming a victim of double-extortion ransomware.

If you would like to submit a question to our panel in advance of the webinar, please contact vgomez@mks.co.uk

Date	Thursday 18 March 2021
Time	16:00 – 17:00 GMT
Speaker Panel	• Maritz Cloete, Director of Cyber Security, ClearComm • Dan Faram, Security Consultant, ClearComm
Location	Online – Zoom

CLICK HERE TO REGISTER

NOT FOR PROFIT 2021 WEBINAR PROGRAMME

Our webinar programme covers a wide range of topics. For further information on all our webinars, please visit www.mks.co.uk/events

CONTACT US

Janice Riches
Head of Trade Associations & Membership Bodies
@ jriches@mks.co.uk

Andrew Stickland
Not for Profit Partner
@ astickland@mks.co.uk

Luke Holt
Not for Profit Partner
@ lholt@mks.co.uk

City
Devonshire House
60 Goswell Road
London
EC1M 7AD
t: +44 (0)20 7566 4000

Heathrow
The Shipping Building
The Old Vinyl Factory
Blyth Road, Hayes
London UB3 1HA
t: +44 (0)20 8848 5500

Redhill
Betchworth House
57-65 Station Road
Redhill
Surrey RH1 1DL
t: +44 (0)1737 779000

Romford
Orbital House
20 Eastern Road
Romford
Essex RM1 3PJ
t: +44 (0)1708 759759

St Albans
4 Victoria Square
St Albans
Hertfordshire
AL1 3TF
t: +44 (0)1727 896000

West End
Charlotte Building
17 Gresse Street
London
W1T 1QL
t: +44 (0)20 7304 4646

Join us on LinkedIn Follow us @mooreksllp Brexit Hub Coronavirus Hub

MOORE Kingston Smith

www.mks.co.uk/sectors/trade-associations/