WORKMATTERS
The natural choice for human resources

NEWSMATTERS

July 2017

In This Issue

Changes in the Law:

WELCOME TO THE THIRD NEWSLETTER FOR 2017

Our newsletter is issued to you quarterly to ensure that you can be kept up to date with employment issues. We will offer helpful hints on how to handle situations within the workplace, but never be afraid to give us a call for both guidance and support. All newsletters are on our website ensuring easy access to current information just click on the newsletter you wish to view.

This Quarter the focus is on the changes in law which may affect your business.

- National Minimum Wage changes took place in April 2017 make sure you are compliant
- General Data Protection Regulation coming into force May 2018 get ready!
- How to avoid the Employment Tribunal

We think you'll find the articles very interesting. Please call us on **01442 870742** to discuss any of these articles and see how we can help you and your business more effectively in the field of Human Resources. Alternatively have a look at our website **www.workmattershr.co.uk** and email us from there or on **carolinebrode@gmail.com.**

If you would prefer not to receive any future newsletters from Work Matters (HR) Ltd, please reply to this email with 'unsubscribe' in the title and we will remove you from our list – thank you.

Work Matters (HR) Ltd Amberley, 18 Oakwood, Berkhamsted, Herts HP4 3NQ
T 01442 870742 M 07711 613153 E info@workmattershr.co.uk W www.workmattershr.co.uk

CHANGES IN THE LAW

National Minimum Wage

From 1 April 2017 the rates for the national minimum wage rose as follows (figures in brackets show the previous rate):

Workers aged 25 and over: **£7.50** (£7.20)

Workers aged 21 to 24: **£7.05** (£6.95)

Workers aged 18 to 20: **£5.60** (£5.55)

Young workers aged under 19 but above compulsory school age who are not apprentices: **£4.05** (£4.00)

Apprenticeship rate: **£3.50** (£3.40)

National living wage

The national living wage for workers aged 25 and over came into force last year, on 1 April. At the time, the government announced that its target was to increase the national living wage to £9 an hour by 2020.

The national minimum wage was previously uprated every year in October but, from 1 April 2017, all national minimum wage rates including the national living wage will be uprated at the same time.

The national living wage should not be confused with the 'Living Wage' or 'London Living Wage' which is an entirely voluntary hourly rate of pay promoted by the Living Wage Foundation. It is set independently and updated annually to reflect the basic cost of living in the UK.

Penalties and non-compliance

Employers need to ensure that they comply with the new rates as the penalties for failure to do so are now significant: 200% of arrears (halved if employers pay within 14 days) up to a maximum penalty of £20,000 per worker.

Many examples of non-compliance are not intentional but occur as a result of administrative failings. For example, employers need to make sure they have the correct systems in place to identify when workers have a birthday and move from one rate to another.

General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR), which applies to all member states from 25 May 2018, will also apply here, even though the UK is leaving the EU.

The regulations provide individuals with easier access to their own data, a 'right to be forgotten', and a right to know when their data has been hacked. There will be one set of rules applying across all EU member states, and one supervisory authority rather than the current individual authorities in each country. Organisations may need to appoint a data protection officer, and could face a fine equivalent to 4 per cent of their global turnover if they breach the rules. Exemptions apply for SMEs for whom data processing is not a core business activity.

The Information Commissioner's Office has produced a 12-step guide to the new rules.

Step 1 - Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one. Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations. You may find compliance difficult if you leave your preparations until the last minute.

Step 2 - Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within particular business areas. The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

Step 3 - Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation. When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under

Work Matters (HR) Ltd Amberley, 18 Oakwood, Berkhamsted, Herts HP4 3NQ
T 01442 870742 M 07711 613153 E info@workmattershr.co.uk W www.workmattershr.co.uk

CHANGES IN THE LAW continued...

the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language. The ICO's Privacy notices code of practice reflects the new requirements of the GDPR.

Step 4 – Individual Rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format. The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy.

This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion? The right to data portability is new. It only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

You should consider whether you need to revise your procedures and make any changes. You will need to provide the personal data in a structured commonly used and machine readable form and provide the Preparing for the General Data Protection Regulation (GDPR):

Step 5 – Subject access requests

You should update your procedures and plan how you will handle requests to take account of the new rules:

- In most cases you will not be able to charge for complying with a request.
- You will have a month to comply, rather than the current 40 days.
- You can refuse or charge for requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy.

You must do this without undue delay and at the latest, within one month. If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

Step 6 - Lawful basis for Processing Data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it. Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing. You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. It should be possible to review the types of processing activities you carry out and to identify your lawful basis for doing so. You should document your lawful bases in order to help you comply with the GDPR's 'accountability' requirements.

Step 7 - Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard. You should read the detailed guidance the ICO has published on consent under the GDPR, and use our consent checklist to review your practices. Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, preticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Public authorities and employers will need to take particular care. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data. You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

Step 8 - Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity. For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services ('information society services') to children and relies on consent to collect information about them,

CHANGES IN THE LAW continued...

then you may need a parent or guardian's consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding 'parental responsibility'. This could have significant implications if your organisation offers online services to children and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

Step 9 – Data Breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach. Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases. You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Step 10 – Data Protection by Design and Data Protection Impact Assessments

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR. You should therefore start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally? You should also familiarise yourself now with the guidance the ICO has produced

on PIAs as well as guidance from the Article 29 Working Party, and work out how to implement them in your organisation. This guidance shows how PIAs can link to other organisational processes such as risk management and project management.

Step 11 – Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer (DPO). You must designate a DPO if you are:

- a public authority (except for courts acting in their judicial capacity);
- an organisation that carries out the regular and systematic monitoring of individuals on a large scale; or
- an organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions.

The Article 29 Working Party has produced guidance for organisations on the designation, position and tasks of DPOs. It is most important that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively.

Step 12 International

If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority and document this. The lead authority is the supervisory authority in the state where your main establishment is. Your main establishment is the location where your central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented. This is only relevant where you carry out cross-border processing – ie you have establishments in more than one EU member state or you have a single establishment in the EU that carries out processing which substantially affects individuals in other EU states. If this applies to your organisation, you should map out where your organisation makes its most significant decisions about its processing activities. This will help to determine your 'main establishment' and therefore your lead supervisory authority.

HOW TO AVOID THE EMPLOYMENT TRIBUNAL

The Employment Tribunal (ET) is hardly a destination of choice and there is much to be said for not having to spend much time there. Often a Tribunal case ends up being fought with Barristers and heavy weight legal teams which issue bills which can run into their thousands as an organisation it is imperative to decide is it worth it?

Small / medium sized businesses often don't have the benefit of an HR team focused on claim prevention. This can be a factor in employment problems not being nipped in the bud at an early stage and matters escalating, until an appearance at the employment tribunal begins to look inevitable. Using independent HR firms may in the long term help avoid massive costs.

There are many ways that small / medium sized businesses can avoid costly employment claims. The following examples are some of the most common employment issues that small businesses may face:

Employment contracts

There are no valid excuses for not having employment contracts and policies in place. Employees have a right to receive written terms and conditions of employment and certainty over employment terms and this is good for both the employer and the employee. As an employer you have 8 weeks in which to issue full terms and conditions.

Ambiguity over notice periods, working hours and job roles simply leads to more problems in the long run. Employment contracts can include useful terms, such as the right to pay an employee in lieu of notice if things are not working out, and restrictive covenants to protect against competition and poaching of clients.

Employment policies

Employment tribunals are rarely impressed when an employer facing a discrimination claim has no equal opportunities policy. Ditto in a whistleblowing case.

Employment contracts should state where an employee can access disciplinary and grievance procedures. Employers which have policies are in a better position to manage their workforce, which means that problems are tackled head on before they turn into claims against the organisation.

Employment policies should be regularly reviewed and updated and be readily available to employees. Generally, they should not be contractual and are more for guidance in line with best practice.

Taking the time to put together a staff handbook of basic policies will pay dividends in the long term.

Poor performance

A reluctance to deliver difficult messages and a head-in-sand approach towards poor performance spells trouble. To ensure that employees are achieving targets and objectives, performance should to be reviewed on a continuous and regular basis.

Small businesses may find it helpful to develop an appraisal system to identify where improvement is needed. A paper trail is key.

Do not use this process as an opportunity to berate your employee this is not a disciplinary but should be a positive experience for both parties, should there be a problem separate it away from the review and hold a disciplinary instead.

Flexible working: While employees do not have the right to work flexibly, there is an obligation on employers to deal with requests in a reasonable way and not to reject them out of hand without reference to a business rationale.

There are few jobs that cannot be done more flexibly today and a family friendly workplace is likely to be seen as a more attractive option, encouraging better retention rates and loyalty. Special care should be taken in dealing with female employees with childcare responsibilities to stay on the right side of the sex discrimination legislation.

Sickness: Employers need to ensure that they handle sickness issues sensitively, both while the employee is off from work and when they return. Sick pay policies should be managed in a consistent way, especially when there is an element of discretion about whether to pay more than statutory sick pay.

Employers should be alert to the need to stay on the right side of disability discrimination legislation and make reasonable adjustments for employees with disabilities. A disability may not be tangible so a cautious approach is recommended.

The benefits of getting things right from the start in employment law terms cannot be overstated. The cost and management time of defending an employment tribunal claim can have a big impact on a small business. Prevention is certainly better than cure.

Thank you for taking the time to read our Newsletter which I hope you found informative An e-newsletter will be sent on a quarterly basis to help keep you up to date with current legislation changes, as well as giving you some helpful hints and tips to help your business run smoothly.

In the meantime please contact us if we can be of service to you or your company.

Have an enjoyable quarter and we look forward to issuing you with our next newsletter in the early part of October 2017 following the referendum and highlighting how this has affected you as employers.

Work Matters (HR) Ltd Amberley, 18 Oakwood, Berkhamsted, Herts HP4 3NQ
T 01442 870742 M 07711 613153 E info@workmattershr.co.uk W www.workmattershr.co.uk