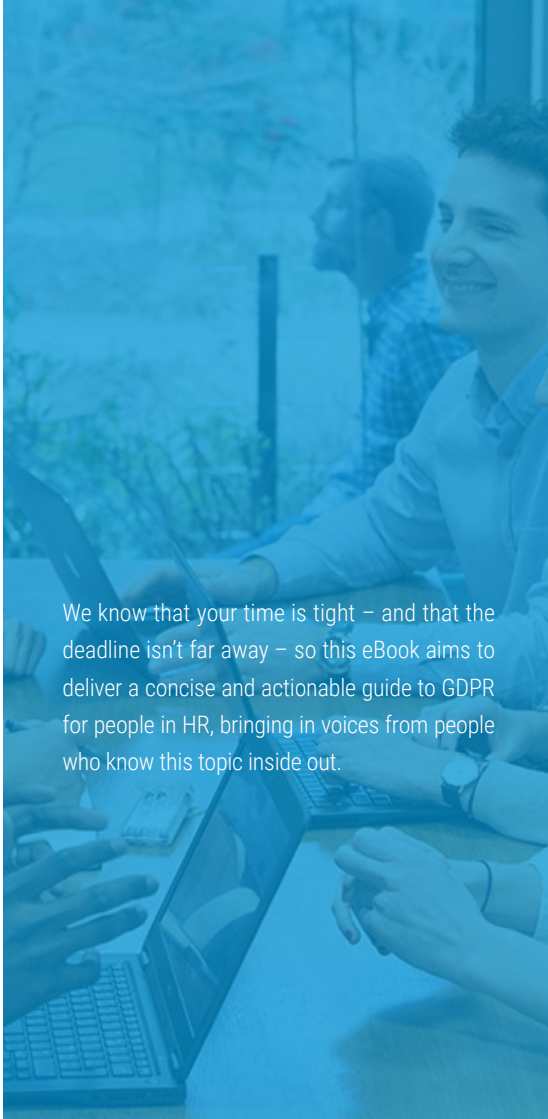
TALENTSOFT

THE ESSENTIAL **GDPR GUIDE FOR *HR DIRECTORS***

What you need to know about
the new data rules

CONTENTS



We know that your time is tight – and that the deadline isn't far away – so this eBook aims to deliver a concise and actionable guide to GDPR for people in HR, bringing in voices from people who know this topic inside out.

01

GDPR: *WHAT IS IT?*
WHY IS IT BEING INTRODUCED?
IS YOUR HR DEPARTMENT *READY?*

WHAT IS GDPR?

Ok, so we know that most of you will have heard about GDPR by now (some of you will have heard a lot), but it's worth taking a quick step back, considering what this is and why it is being introduced before we dive deeper into how it might impact on your job on a day to day basis.

GDPR stands for Global Data Protection Regulations and refers to a new set of rules drawn up by the European Union. The aim here is to replace existing legislation, such as the Data Protection Act 1998 in the UK, and bring legislation up to speed with the current digital landscape.

The rules come into force on May 25, 2018. Simple as that.

"GDPR is a natural evolution of the Data Protection Act to embrace the technological age that we live and work in so see this as an opportunity to revisit documentation and processes in an effort to improve what we do and why we do it. This is a good thing."

Martine Roberts, **director of HR consulting company HR Dept**

This last point is an important one. HR departments – and, indeed, businesses as a whole – need to embrace GDPR as a positive change. It creates higher standards for the collection and handling of data.

Reaching those higher standards means companies will have to get explicit consent to be able to collect, store and process data belonging to individuals. If that isn't obtained, you'll need what's known as an 'alternative lawful basis'.

SO, WHAT'S THIS GOT TO DO WITH HR?

Well, with data on employees – past and present – and job candidates, people working in HR are swimming in a sea of data and will be at the front line when it comes to ensuring businesses are GDPR compliant and, therefore, not facing fines (more of that later).

To their credit, people in HR know full well that this is pretty important. A survey of 550 HR professionals by the Chartered Institute of Personnel and Development (CIPD), conducted at the end of 2017, revealed that almost half of respondents saw this as their main concern for 2018.

HR departments have GDPR on their radar, therefore, but are they ready to go? After all, the clock is ticking and that May 25 deadline is fast approaching.

Almost half of HR professionals surveyed saw GDPR as their main concern for 2018

Roberts reckons HR departments in the UK have been ready for this change for some time – but were helped in their quest to get their wider businesses to sit up and take notice when the Information Commissioner's Office issued advice on what this would mean in practice with a 12 point guide last May (see this here). Most people in HR will probably appreciate the challenge involved in getting the rest of the business to sit up and take notice. She said:

"Generally, my experience is that the HR community has been taking this seriously for the last year but clarity from the ICO was needed… before tangible action could be undertaken."

Ed Boal, head of digital media and technology at law firm Gregg Latchams, believes that HR professionals are well suited to this change as they are well versed in sensitively handling data, but they will still need to change their mindset. He said:

"I think HR departments, perhaps more than other departments, appreciate the importance of data protection and respecting the rights of individuals in relation to their personal data. However, HR departments often process more personal data than they first realise and identifying all of the categories of personal data they handle, the purposes they are processed for and the lawful grounds for doing so can be a considerable task."

02

HOW WILL GDPR *CHANGE THE WAY* HR PROFESSIONALS WORK?

HOW DOES THIS APPLY TO ME?

Are you sitting there and wondering if all this applies to you? Let's answer that for you. GDPR is something that all businesses (including the self-employed) need to be aware of if they are processing data for individuals living in the EU. This is the case regardless of whether or not the company is actually based in the EU too.

If you are struggling to get the wider businesses to take this seriously, the potential cost of breaking the rules really ought to help.

Failure to keep up with GDPR could lead to a fine of up to 4% of the annual turnover of your business or up to €20 million, whichever is highest.

AVOIDING A FINE

It isn't just about money either. Businesses also shouldn't ignore the fact that a failure to comply with the rules will also potentially damage the reputation of your company too – and no organisation wants to appear as playing fast and loose with personal data, not least when this issue has risen to the top of the news agenda in recent times. Customers and clients have clocked on to this issue now – you're dealing with a more clued up world when it comes to data.

So, the looming threat of a fine should focus minds but what will HR professionals be doing to avoid this?

01 | *You may need to get consent from employees to process their data*

One word to keep in mind at all times when it comes to GDPR is consent. The biggest cultural change brought about by GDPR is the need for consent when it comes to using data. Previously, companies have written a broad brush statement into the contracts of their employees outlining that they consent for their data to be processed but GDPR now sets out that this must be 'freely given, specific, informed, and clearly indicated'.

There are two ways for HR professionals to react to this. Firstly, they will need to be much more explicit about the data they will process and why. Secondly, they might well be able to rely on the 'other lawful basis' for processing data, given that employers can be expected to lawfully require to do this. However, HR professionals cannot assume that this gives them free reign to continue as before (hence the need to be more explicit in the first instance) and they must be careful to ensure that the data they process does fall within their legal obligations.

AVOIDING A FINE

It's worth noting that this 'lawful basis' will let you carry out processes that are necessary for complying with a contract or the law. So, for example, you need someone's bank details to pay them or details of their right to work in a given country to prove they are lawfully employed, for example. However, this should occur 'except where such interests are overridden by the interests, rights or freedoms of the data subject'.

02 | *You need to report a data breach*

HR professionals will have a duty to report any personal data breaches that occur. GDPR sets out that the appropriate bodies must be notified of such breaches within 72 hours. In the UK, for example, this means alerting the Information Commissioner's Office. If this isn't possible, a reason must be given for failing to meet the deadline.

GDPR sets out that the appropriate bodies must be notified of a breach within 72 hours.

So, for example, losing a laptop, phone or memory stick that contained employee records would have to be reported, as would an email containing private data that was sent to an incorrect email address.

03 | *You have to respond to access requests*

The current data protection rules do give people the right to request all the information held on them. However, the way in which such requests are processed will need to change.

For instance, under current laws in the UK data subjects are charged £10 and their requests need to be fulfilled within 40 days. Under GDPR, this will need to be done quicker. The rules state a request should be made 'without undue delay', with a deadline of a month. This could be extended if the request is particularly complex, but the data subject will need to be informed of an extension and be given a reason within the month deadline. On top of this, there is no charge for carrying out this request (unless it's deemed excessive).

AVOIDING A FINE

04 | *You need to be aware of the new rights*

The right to these enhanced subject access requests is one of a bundle of new rights introduced by GDPR. While many rights carry forward from the current rules, it's important to note that there are changes here.

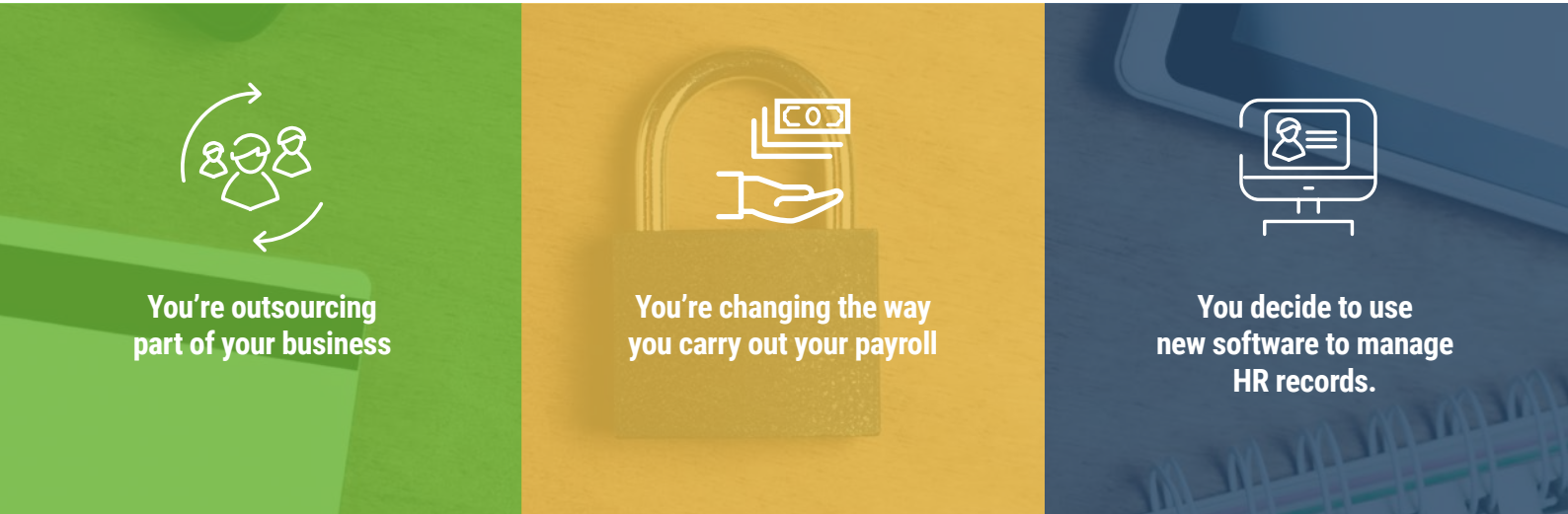
The concept of 'data portability' is new to GDPR. It essentially means that people have the right to obtain and reuse their personal data, meaning they can copy and transfer this from one IT system to another.

AVOIDING A FINE

04 | *You need to promote privacy*

It's time to get passionate about privacy. GDPR calls on you to actively promote privacy and data protection compliance. For people in HR, this could mean carrying out Privacy Impact Assessments if:

The key thing here is to make sure the 'p' word comes into the conversation at all levels of your business. Companies might be used to thinking about cost, efficiency and quality, but not so much privacy and that needs to change. Regular Privacy Impact Assessments can bring that to the table.



You're outsourcing part of your business

You're changing the way you carry out your payroll

You decide to use new software to manage HR records.

03

THE KEY THINGS FOR HR PROFESSIONALS *TO CONSIDER*

WHAT YOU ACTUALLY NEED TO DO

Obtaining consent, reporting breaches, reflecting new rights, promoting privacy and responding to access requests must all be part, therefore, of a GDPR compliant HR department. But it's all well and good talking about these things, how do you actually achieve them? No it's time to think about what you actually need to do…

Audit your data and your processes

You need to have an accurate picture of the state of play right now before you think about any changes. What data do you hold, where did you get it from, how did you get it, who has access to it and what do they use it for? When did you get consent, how was this given and where is the record for this?

This will allow you to have a little spring clean of your data – removing any information that you collected and don't need. It'll also force you to spot any processes that you need to update or any data consent that needs revisiting to meet the new regulations. Keep a record of the audit you carry out too, this might be important to demonstrate the work you've done if this is later questioned. You do not have to automatically go through and refresh consents, but if your current practices do not meet the standards set out by GDPR then this does need to happen.

Update your systems to comply with the new rules

As you'll no doubt have noticed, there's a fair amount of record-keeping required when it comes to GDPR and HR. There's no getting away from that, but there's no reason why you can't make that easier. You might well need to update your processes so that you are able to accurately record the data you've obtained and when and how you obtained consent for acquiring this. Your systems also need to be able to cope with removing data once you no longer require it (individuals should be clear about how long you'll hold their data too) and to respond once a request is made. For some businesses, that might prompt a software review, especially if you hold different data sets in different places and would struggle to react swiftly enough to a subject access request.

WHAT YOU ACTUALLY NEED TO DO

It's likely that you'll need to update some of your paperwork too. If your current contracts contain a section designed to obtain consent, this should be reviewed. GDPR requires consent to be indicated in a clear and positive way and for a specific reason. That means you can't bundle together several different data uses in one statement, present a pre-ticked box on a form or assume consent because an individual hasn't opted out or said 'no' to a request.

Finally, you might need to update your personnel. Businesses carrying out large scale monitoring or processing of data are required to appoint a Data Protection Officer (DPO) to take responsibility of the work required by GDPR. If your business doesn't directly require a DPO, however, you may still wish to allocate responsibility for this to one person who can act as a point of contact for everyone in your organisation.

GDPR requires consent to be indicated in a clear and positive way and for a specific reason.

Training to get your staff GDPR-ready

People in HR departments might be well-versed in data management and ideally placed to cope with GDPR but any business is only ever as strong as its weakest link. One slip up by one person could cause you to suffer the sort of penalties we've discussed earlier in this eBook.

It's important, therefore, to make sure everyone who handles data is given training to ensure they understand the new rules and how to comply with them.

Plus, while this book should hopefully prove useful, it's likely that you and your business will have specific questions and requirements to consider as part of the new rules. With this in mind, it's important that HR teams get sound legal advice and training with people who can address any particular concerns they have.

WHAT YOU ACTUALLY NEED TO DO

Patrick O'Kane, a lawyer and Data Protection Officer for a US Fortune 500 company and the author of GDPR: fix it fast, told us:

"Your employees are crucial to your business but can often be the weakest link in data security processes – one study found that staff error was the cause of 37% of data breaches. You need to ensure that all your employees are trained on data protection and their responsibilities under GDPR. Some staff will only need to know the basics but specialists may need further training related to their role. For example, HR will need to know more about the new data rights under GDPR, so they can deal with requests from employees to assert those rights."

One study found that staff error was the cause of 37% of data breaches

Patrick O'Kane

WHAT YOU ACTUALLY NEED TO DO

Communication is key

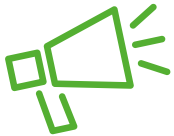
Finally, make sure you pay close attention to communication. You need to think about how you will tell everyone in your business about GDPR. Don't lecture people for hours on the finer points of the legislation, but do make sure they're aware that this isn't just a side issue that they don't need to know about.

Iain Jenkins, Blacks Solicitors Employment Director, said:

"The biggest challenge is probably getting employee engagement across the organisation. A common misconception is that GDPR is just about IT security. Successful GDPR compliance really requires employee engagement across the organisation, including an understanding of the organisation's obligations in relation to data processing and what constitutes a data breach."

Charles Cotton said that this is about creating an ***'appropriate workplace culture'*** so that GDPR compliance becomes an ***'unconscious habit'***.

Making sure people know about GDPR, how to report any issues they have with this and, crucially, who to report them too, is going to be an important part of the process of getting your business to be GDPR-compliant. That's why clear channels of communication are vital for any business.



EXPERT OPINIONS

We've heard above from some experts on the key things that people in HR need to consider. Here's some insight from three more professionals, who tell us what they consider the key challenges facing HR departments to be:

"Making sure that the employment documentation is updated and that privacy notices are generated and tailored to avoid falling foul of GDPR! Getting people trained in how to handle this appropriately takes considerable time and effort. More importantly, trying to get businesses to realise that its everyone's responsibility and not just HR is often the biggest challenge. I recall that from the Data Protection Act 1998!"

Martine Roberts

"The hardest part is probably data mapping, no matter how old the data is."

"Employee data (and there's going to be a lot of it) needs to be kept on a secure system. HR managers need to be able to access this data and supply it to a past or present employee should they ask for it. I think the hardest part is perhaps the data mapping, no matter how old the data is. To be compliant the HR team will need to record where the data has come from, who or what system the data passed through, where it is kept and who has access to it. That is potentially a huge job to map this process."

Ben Leach

"I think the biggest challenge is ensuring compliance with the GDPR in relation to HR matters day-in-day-out. It can be an incredibly busy role which often requires quick thinking – for example, setting up a WhatsApp group to communicate with employees during adverse weather conditions is a practical idea, but sharing employees' phone number with a third party without asking the employees if they were ok with this is not. Maintaining confidentiality within a busy corporate environment is also often easier said than done."

Ed Boal

04

HOW TO BE *GDPR READY*

GDPR AND HR: THE CHECKLIST

Once you know what needs to change as a result of GDPR and how to go about changing it then you can feel confident about keeping up with the new requirements.

However, before you go off and do anything, here's a handy checklist of the questions to answer before you begin – and then a few insider tips from our six GDPR experts on the key things to implement in your business.

- o **Are you clear on what GDPR is and what the penalties are for failure to comply?**
- o **Does everyone in your business know the deadline and what they need to do to be ready for this?**
- o **Are you clear on how to obtain consent and keep a record of this?**
- o **Are you confident that you know how to respond to subject access requests?**
- o **Do you have a plan in place to report data breaches?**
- o **Do your systems promote privacy and data compliance?**
- o **Are you clear about all of the rights covered by GDPR?**
- o **Have you conducted an audit of your data and data capture processes?**
- o **Has key paperwork such as employee contracts been updated to reflect GDPR?**
- o **Have you appointed a DPO – or nominated a key contact in your business to co-ordinate GDPR activity?**

- **Are you and your staff fully trained and confident about how GDPR affects your business?**

- **Do you have a clear communication strategy in which everyone knows how to report any issues and who to report them to?**

If you can answer 'yes' to all dozen of those questions then you're in a pretty good place. If not, then you know where your efforts need to be concentrated between now and May 25.

Having appropriate staff data protection policies in place is vital to GDPR compliance

Patrick O'Kane

WHAT DO OUR EXPERTS RECOMMEND?

Here's their advice on what you can do right away to stay on top of this:

Iain Jenkins

"My top tip is to have a comprehensive communication strategy, which includes all employees and make sure that you have provision for employee training. A regular reminder about GDPR and its implementation will keep it at the forefront of everybody's mind. If you are not required to formally appoint a Data Protection Officer then there should also be someone in the organisation at an appropriate senior level who has responsibility for compliance."

Patrick O'Kane

"Having appropriate staff data protection policies in place is vital to GDPR compliance. Companies and public bodies must have appropriate 'accountability' in place around GDPR. That means making sure that staff know what the rules of the game are when they are handling personal data. Dusty old staff policies that were never read, much less acted on, will be a thing of the past. You must have practical and easy-to-understand staff policies in place that help educate and inform your staff about how they should be handling personal data."

Martine Roberts

"Also I would recommend retaining H&S and auto enrolment data ongoing beyond the statutory timelines as there is a danger that this could be destroyed in order to comply with GDPR. The latter is likely to bring issues in a few years' time when people realise that auto enrolment contributions perhaps have not yielded the pension pot they expected and this is highly likely to result in claims against employers so don't get caught out."

WHAT DO OUR EXPERTS RECOMMEND?

Charles Cotton

"As data protection law is a highly technical area and the cost of breaches could be large, not only financial but reputational, it's worth seeking out the appropriate legal and good practice advice and guidance at the outset."

Ben Leach

"I'd say that it's important to understand the security behind where your data is being kept. As time consuming as it is, an audit of your software may be required. But rule number one? Don't panic."

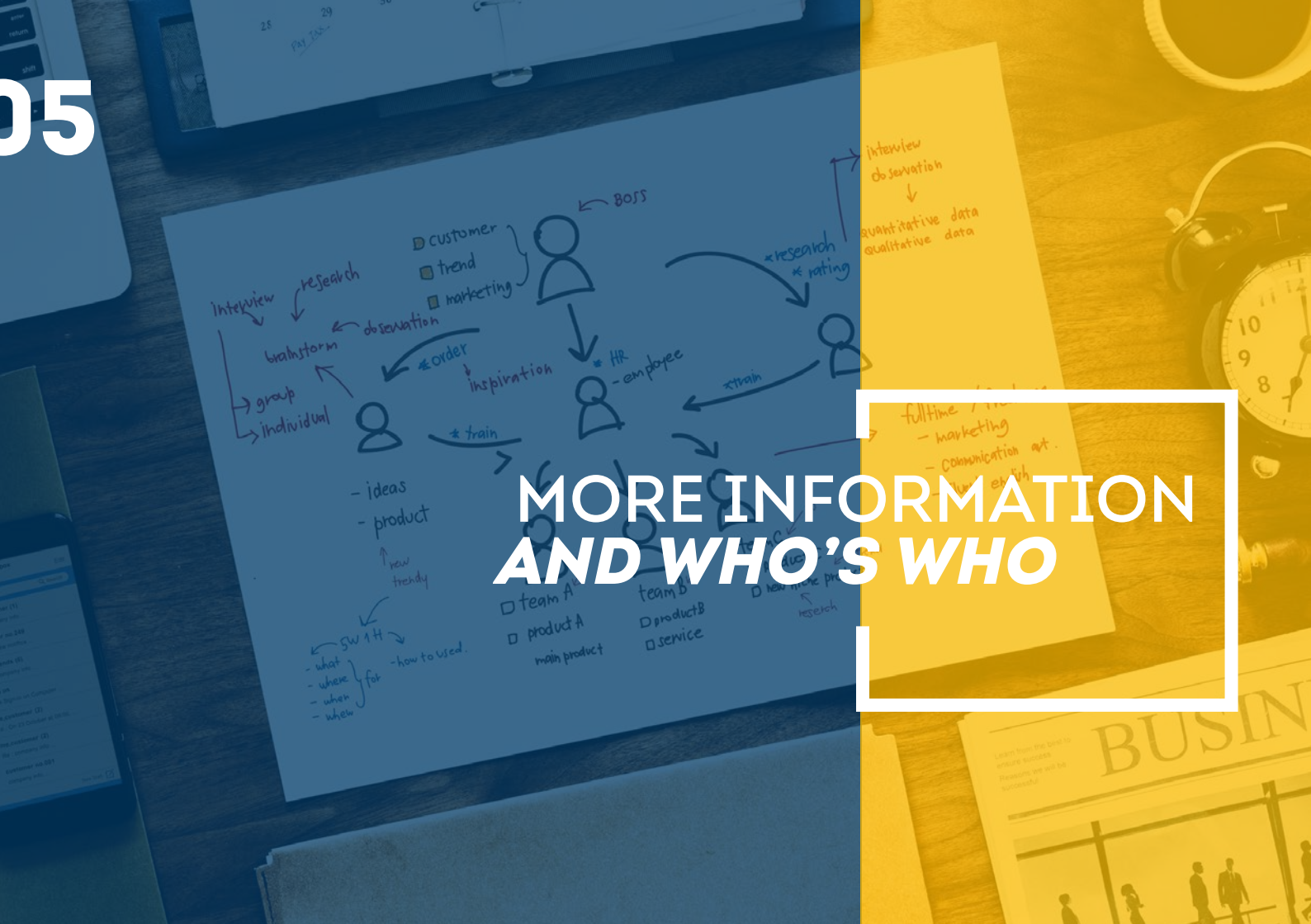
Ed Boal

"Asking the question: "Do I need to really ask for/know this information?", can avoid any number of nasty data protection issues and also help the organisation to comply with its equality obligations."

Rule number one? Don't panic.

Ben Leach

05



MORE INFORMATION *AND WHO'S WHO*

READ MORE ABOUT GDPR

If you want to read more about GDPR then it's important to stick to reputable sources to avoid some of the scare stories. Some people are always daunted by change but, as we've seen, a few tweaks to your practices and workplace structure should be enough to help you to become compliant and ensure you embrace rules that reflect the business world we're all operating in.

If you want to know more, we'd recommend talking to a legal advisor or turning to one of the following sources:

Slaughter & May's guidance: An informative and easy to digest guide on GDPR, consent and legitimate interest from a respected legal specialist

ICO's helpline for small business & charities: A highly useful resource for companies with limited resources

The ICO's full guide to GDPR: If you really want to drill down to the detail, it's all here.

OUR EXPERTS

Thanks to the following people for offering their insight into this eBook.

Charles Cotton is **performance and reward adviser for Chartered Institute of Personnel and Development** (CIPD) the professional body for people in HR.

Martine Roberts is **director at HR Dept**, a specialist which helps to provide advice and support on all matters HR.

Ben Leach is a **digital marketing and PR executive for HeX Productions** – a web design and maintenance company – with a keen eye for what GDPR means in practice.

Ed Boal is **head of digital media and technology at law firm Gregg Latchams**, with experience in everything from securing investment to the development and licensing of technology platforms and privacy and data protection matters.

Patrick O'Kane is a **lawyer and data protection officer for a US Fortune 500 company** and is also author of the book GDPR: fix it fast.

Iain Jenkins is **employment director at Leeds-based law firm** Blacks Solicitors and is advising clients on the impact of GDPR.

TALENTSOFT

ABOUT TALENTSOFT

Talentsoft's cloud-based technology offers a market-leading solution to help keep your employees happy. Our software is ideally placed to ensure you are able to comply with GDPR because it:

- Includes ready-made product features to naturally cover the right to be deleted and the right to access
- Includes a full risk analysis and protection plan in place
- Features privacy by design and by default
- Protects information in highly secured data centres in the EU

All of our administrators are based in the EU, so data does not have to travel across borders or to the US or any other overseas destination. Talentsoft is ISO 27001 certified and can demonstrate GDPR compliance with a thorough and transparent process.

Tel. +45 58 51 50 95 • contact.dk@talentsoft.com

WWW.TALENTSOFT.DK