CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

Human Resources

Handling Employee Data: What You Can and Can't Do with your Employees' Data

Tom Andrews

Tom Andrews
Founder and CEO
Rightly

Biography

Tom Andrews is the Founder and CEO at Rightly (https://www.rightly.co.uk). In 2018, Tom founded Rightly because he saw an opportunity to use the new consumer legislation and protection on personal data to help people understand what's happening to their data – and take control of it. Launching in May 2020, Rightly has already helped over 60,000 people and works with 12,000 firms.

Attending university at Imperial College, London, Tom graduated with a Bachelor of Science (BSc) in Physics. He has always been analytically minded and after university he followed a career in problems solving for businesses like KPMG and PwC, focused on financial markets, risk assurance and forensic accountancy.

Keywords Personal data, Employee, Human resources, Management, Compliance, General Data Protection Regulation (GDPR)
Paper type Research

Abstract

The Human Resource department holds a lot of personal information about the organization's employees, from details of any medical conditions, through to salary and bank account details. Some might say, with great information comes great responsibility. That is why it's important to develop a culture in the workplace of respect for private life, data protection, security and confidentiality. Not only to keep in line with General Data Protection Regulation (GDPR) and data protection, but as the author of this article explains, taking care of employee records for good data protection practices, also has a knock-on effect of improving business more broadly – and in a very positive way.

Introduction

Managing employee records whilst adhering to strict data protection practices remains a key factor in human resource management. Done well, it becomes part of a strategic and comprehensive approach to managing people and the workplace culture, creating an environment that enables employees to contribute effectively and productively to the overall company direction and the accomplishment of the organization's goals and objectives. So, it is more important than ever to know how to properly take care of your employee records and get all the benefits from good data protection practices.

What is employee personal data?

By its very nature 'personal data' refers to any information that can be used to identify a certain employee, such as:

- Name
- Financial details
- Address
- Relationship status
- Health records

It also includes any emails involving a named employee and sick leave records. This includes automated and computerized personal information, paper records or any organized 'well structured' filing system.

By 'employee' this also means data on any potential employees (job applicants); current and former employees; agency staff; casual or part-time staff; and contractors.

Benefits of protecting employee data

When employers implement good data protection policies and practices in the workplace, the rewards include:

- Increased trust in the company as a result of a more transparent environment;
- Increased efficiency by deleting out-of-date information and freeing up filling systems so that important information is easier to find; and
- by making employees aware of the importance of data protection, employers can avoid expensive legal action.

But what data can be processed without an employee's permission?

You can collect:

- Name, date of birth and National Insurance number to identify employees for background checks or when recording taxes;
- Address;
- Bank account details to pay them;
- Terms and conditions of employment such as salary, leave, benefits and hours;
- Gender to monitor and ensure the equality of jobs offered to each sex;
- Education and qualifications in case an unsuccessful applicant files a discrimination claim for example;
- Accidents at work for your records and in case someone makes a claim against the company;
- Any disciplinary action they have been involved in as evidence in case the employee takes the case to court;
- Emergency contact details.
- Any training that has occurred during employment.

What data cannot be processed without an employee's permission?

You need employee consent before processing any of the following. Usually this is because this data is sensitive and could be used to negatively impact or discriminate against them:

- Health data
- Biometrics
- Religion

- Race and ethnicity
- Trade union membership
- Sexual orientation
- Genetics
- Political membership

Keep in mind that while an employer is allowed to ask an employee to disclose details of their age, sexuality, religion and more in the interests of equality monitoring: the employee is not under any obligation to disclose any of this information if they do not want to.

The dos and don'ts of handling employee data

Generally speaking, how you should process employee data is outlined in these five rules:

1. Process your employee's data in a fair and transparent way.

2. Only collect personal data for specific purposes – don't use it for any other purpose than specified to the employee or in the handbook.

3. Ensure that data gathering is relevant rather than excessive.

4. Keep employee data secure.

5. Only keep personal data for as long as necessary.

As an employer, it’s crucial that you make sure you meet at least one of these six lawful bases for processing set out in Article 6 of the General Data Protection Regulation (GDPR), namely:

1. **Consent:** the employee has given clear consent for a specific purpose.

2. **Contract:** it’s necessary to process data because of a contract with the employee.

3. **Legal obligation:** you need to process in order to comply with the law.

4. **Vital interests:** processing is needed in a life or death situation.

5. **Public task:** processing is needed in the interest of the public.

6. **Legitimate interests:** processing is necessary for your own legitimate interests (unless there’s good reason to believe the employee’s personal interests override these legitimate interests).

Do follow these tips when hiring a candidate

Here are three things you should do when looking for and hiring a new employee:

1. When advertising for a candidate always identify the name of your organization, if it's not obvious inform them of what data you will collect on them, and only ask relevant questions to the application.

2. Inform all employees or applicants if an automated system is being used for example, to shortlist candidates, how they can appeal any decisions made, and always keep the system under review.

3. Vetting should be done minimally and in the least intrusive way. Make sure vetting records are deleted after six months.

Do collect and store employee records carefully

This is where the heavy lifting comes in! At work you may be looking after more data than you realize. Therefore, it is important to notify your employees of the measures you have in place to secure these records, and below are some tips for what you can do to better protect them:

- Consent isn’t usually needed to keep records but notify employees that records are being kept, and remind them of their rights under GDPR.

- When monitoring equality in the workplace ensure the sensitive data isn’t used for any other purposes and that employees have a good range of options in a form for example, for ethnicity monitoring, to accurately identify themselves.

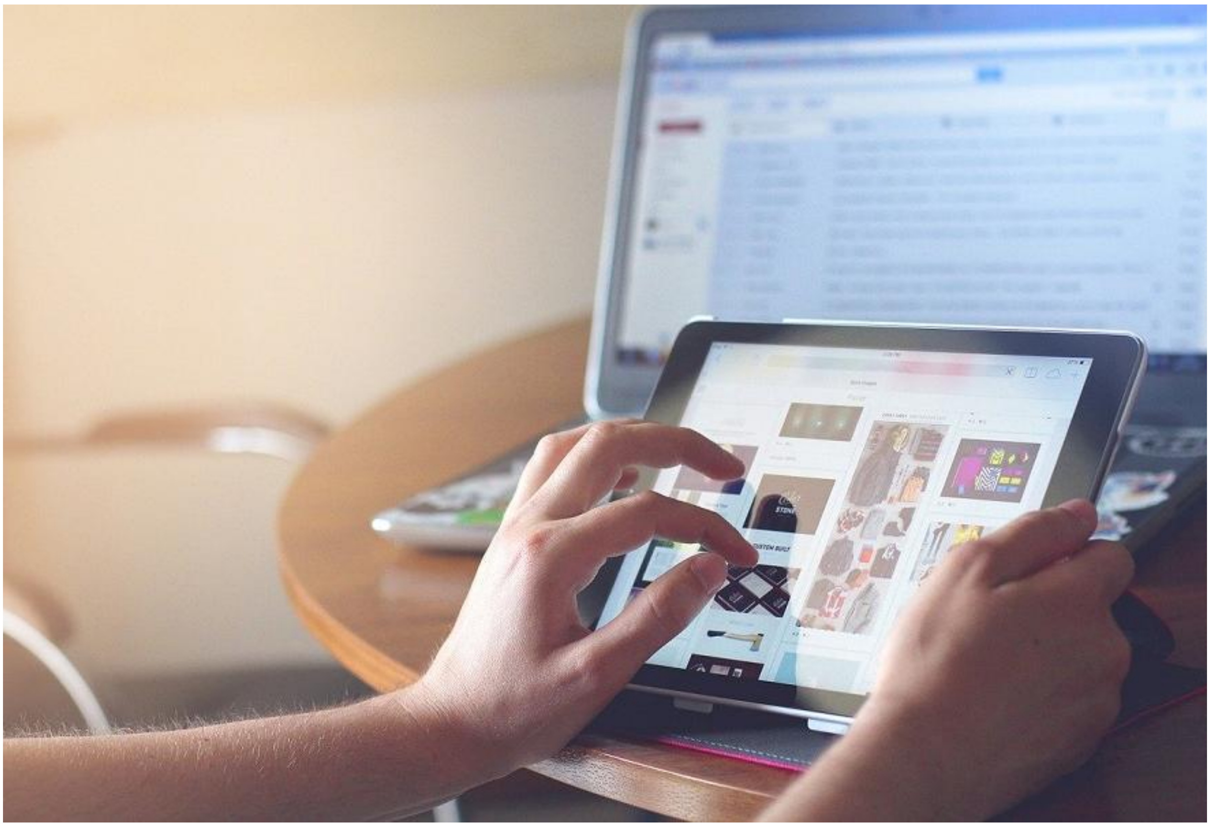
- When detecting fraud inform trade unions or other representatives of proposed data matching exercises, explain how fraud prevention works to any new

CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

employees and don't hand over worker data to outside organizations unless you think disclosing it would prevent a crime.

- When giving references make sure your staff know how much information to give out.
- Ensure that all data requests are valid. To be safe, check the identity of any person making a subject access or deletion request.



Do have good security measures in place

In the unfortunate case of a data breach, loss or destruction, make sure you put in place the security standards set out in the BS 7799: 1995[1]ahead of time. You can read more about exactly what your company should do for security in the code of Practice for Information Security Management guide, but generally it's good practice to do the following:

- Store and transfer any data securely for example, using encryption-based software and making sure access to employee data is limited to only those who need to see it.
- Set strong and unique passwords for yourself and make sure your employees do this, you can use a password manager.

CREDIT CONTROL JOURNAL and ASSET & RISK REVIEW is published by House of Words Media Limited.

The current issue and full text archive of this journal is available at **https://www.creditcontrol.co.uk/**

- Keep track of work devices by warning employees not to leave devices unattended, and encourage them to report lost or stolen mobile devices straight away so you can address it.

Do make sure that your employees handle their own and their colleagues' data well

It's easy to focus on your own data responsibilities, but in reality your employees themselves also handle a lot of personal information, so it is really good practice to make sure all of your employees are aware of how important data protection is. Here are a few tips on how to do this:

- Carry out background checks on staff that have access to employee data for example, by checking references.

- Warn employees not to send personal emails (not related to work) or emails containing rude matters in case they receive a SAR (Subject Access Request). There was one embarrassing instance in a government law office where an employee had to stand up in court and formally admit to sending out emails on their work account that included insulting remarks about another employee. Try and avoid this!

- Train employees well with GDPR. Make sure they know who the Data Protection Officer (DPO) is, as well as how to contact them and what to do if there is a breach.

- Inform interviewers that a candidate may have the right to see their interview notes, and how to store this data.

- Inform staff that when accessing sickness and injury absence records that they don't need to access the full record.

Don't collect excessive information related to employee's health

Health data, that can include maternity leave, disability records or even the results of an eye-test conducted at work using display screens is extremely sensitive. In general, only collect health information if it's needed to protect health and safety, prevent discrimination, or for any other legal obligations.

Explicit consent must be given by employees. To clarify, consent needs to be 'freely given', this can be pretty difficult in a workplace because of the power imbalance between you and the employee, but essentially the employee should be able to say 'no' without penalty and be able to withdraw consent whenever they want. Consent should be 'explicit' by being clear about exactly what health data is collected, why it is being collected, and with whom it will be shared.

Don't collect excessive information when monitoring employees

If you, for example, randomly open up individual workers' emails or listen to their voicemails to look for evidence of malpractice, this can be very invasive to your employee's privacy.

So, make sure your employees are aware of the rules and standards of your monitoring and why you are doing it. Also, don't keep information you collect from monitoring for more than six months if possible. The important thing to do is to conduct an impact assessment.

Do carry out an 'impact assessment' when collecting health data or monitoring employees

As you might think, collecting employees' health data and monitoring them can be extremely invasive. You can't therefore just do it for 'business' purposes, you need to make sure, to a reasonable extent, that the need for doing this processing outweighs your employee's rights to privacy.

To do this, you need to conduct an impact assessment:

- Identify the reason and benefits for collecting health information/monitoring employees;
- Identify any negative impacts of collecting and storing this information;
- Consider any alternatives to collecting health information/monitoring employees; and
- Weigh the benefits against the negative impacts and making a final judgement.

Page 60-63 of the ICO's code[2] has a more in-depth outline of how to conduct an impact assessment. It also tells you why you usually can't rely on employee consent when monitoring them (in this context consent being able to be withdrawn at any time makes this practice difficult).

In conclusion

In the ever changing workplace, data protection compliance should be seen as an integral part of employment practice within an organization. It is important to develop a culture in the workplace where respect for private life, data protection, security and confidentiality of personal information is seen as the norm. By respecting your employees' right to privacy, and demonstrating this by ensuring that the data you collect about them is necessary and securely stored goes a long way to developing a workplace culture where businesses thrive.

Reference

[1] https://www.itgovernance.co.uk/files/Infosec%20101v1.1.pdf

[2] ICO (2011) *The Employment Practices Code.* Available at: https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf