KALLIDUS

Staying GDPR Compliant with an Automated Hiring Process

The GDPR is coming

2018 is a significant year of change for HR. The uncertainty of Brexit and anticipated changes in employment law in response to the Taylor Review requires a more agile approach to talent acquisition. Into that complex mix comes the **General Data Protection Regulation (GDPR)** which comes into force on 25th May 2018, representing the most significant change to data protection laws in two decades.

The new data protection laws will affect how public sector organisations and businesses treat the information relating to customers, their databases and how all employers store and manage the data gathered on their candidates during the recruitment process, especially where automated processes and decisions are used in hiring.

In this eBook **we will look at what the GDPR means** for the recruitment process, the changes to the rights of candidates in relation to data stored by your business and how an ATS can help to support compliance.

The GDPR and the rights of your candidate

One of the most significant changes affecting recruitment processes following the introduction of the GDPR is the impact on the rights of your candidates and the way in which you manage, share and store their data during and after the hiring process.

Broadly, the GDPR relates to two specific areas:

Personal data, i.e. 'name, identification number, location data or online identifier. It also refers to personal data that has been pseudonymised, or key coded where it is easy to link a pseudonym to a specific person.

and

Sensitive personal data. This includes data relating to a person's religious and political views or racial information.

Both areas are relevant to the information gathered on candidate processes, whether manually or through an ATS during the recruitment process.

The GDPR applies to all UK companies which either:

- Employ more than 250 people; or,
- Employ less than 250 people but where data process which affects individuals is 'not occasional' or includes sensitive personal data (which applies to the majority of organisations).

The GDPR also makes it easier for individuals to access the data which your business holds on them. In recruitment this extends to information held on previous unsuccessful job applicants or candidates in your talent pool or data base.

While most businesses are aware of these changes, at the time of writing, up to 60% of UK employers aren't 'GDPR ready' while an estimated one in four are 'GDPR at risk'.

Changes to data management under the GDPR

From 25th May 2018, employers will be required to be more accountable when handling candidate information, particularly in the following areas:

- Details of the information stored on your candidates must be provided, together with the length of time it has been held and what measures have been taken to prevent a security breach.
- A data breach which results in the 'destruction, loss, alteration, unauthorised disclosure of, or access to' that data must be reported to the ICO when that access may have a negative impact on the people it relates to (a breach of confidentiality or financial loss for example).
- The ICO must be informed of any data breach within 72 hours. Candidates affected by this information must also be notified within the same timescale.
- In some cases, organisations may need to recruit an employer responsible for data protection, particularly where 'large scale systematic monitoring of individuals' is being carried out. More details are provided on the ICO website.
- Businesses must also obtain consent to data in certain situations which may require an agreed 'opt-in', specifically during the recruitment process. The ways in which an ATS can support compliance are outlined in the following section.

ICO Guide To The GDPR, Key Definitions
CSO Online : GDPR Requirements, Deadlines & Facts, 3rd January 2018
CIPD, People Management : Employers Are Sleepwalking Into GDPR Abyss, 30th January 2018

The new candidate rights

Once the GDPR has come into force, your candidates may request access to personal information retained on file. That information must be provided within one month from the date of request. At present a £10 administration charge is applied to all requests. Under the new regulation that charge will be abolished, making a higher volume of requests for that information more probable.

The GDPR also permits the 'right to erasure', also known as the 'right to be forgotten'. Candidates can request the removal of data for a number of reasons, including where it is no longer needed for the reason it was collected (i.e. a job application), where there is no reason for holding it (the candidate was rejected), illegal processing of data or if an individual withdraws their consent to it being held.

Recruiters and hiring professionals who wish to continue to retain a candidate on file must obtain that consent.

In summary, the new rules will significantly affect how candidate data is processed, offering candidates the following rights:

- To be notified of a data breach that affects their data within 72 hours.
- To be advised how their data will be used during that recruitment process.
- To transfer that data to another provider (or recruiter).
- To erase all of their details ('right of erasure' or 'right to be forgotten').
- To update or correct the information held on them ('right of rectification').

---

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

The cost of non-compliance

Businesses can be fined for non-compliance with the GDPR for the following reasons:

- Failure to process data correctly.
- Failure to appoint a data protection officer if one is required within your business.
- Failure to prevent a data breach.

Maximum penalties for failure to comply are up to €20 million or 4% of annual global turnover, whichever figure is higher.

Less serious offences risk a maximum fine of up to €10 million or 2% of annual global turnover.

Recruiters and employers with vulnerable data security policies are more exposed to financial penalties and damage to their reputation. In a 'war for talent' your employer brand is often what gives you that competitive edge.

A comprehensive policy that complies with the GDPR reassures both candidates and your clients. With the rise in cybercrime, compliance also offers better protection in the event of a data breach.

How An ATS can help your business comply with the GDPR

The GDPR also specifically affects two specific areas of recruitment processes for employers gathering data on job applicants or potential candidates:

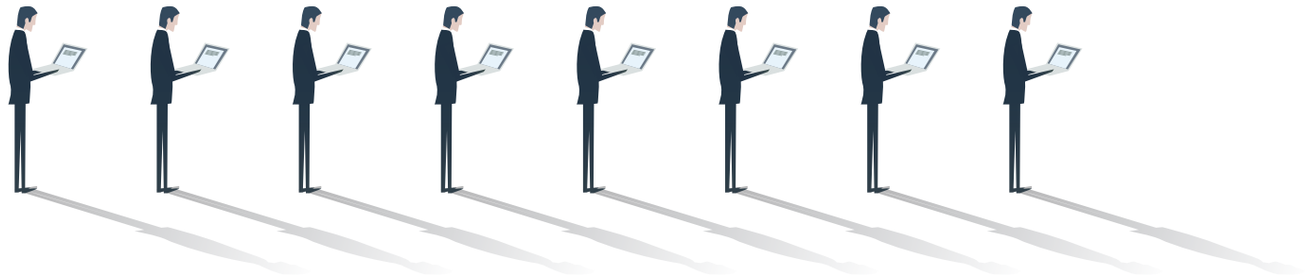
Managing data retention: Candidate data is gathered at numerous points during the hiring process. These range from a simple registration of interest or completed application form to additional pre-hire assessments which may be integrated through your ATS.

Using that information without consent equates to a breach of the GDPR. Explicit consent must be obtained from candidates to their data being used for each stage of the hiring process.

Automated hiring decisions: One of the key rulings for recruiters and HR is focused around the automated processing of data. From 25th May 2018, candidates have the right not to be subjected to a hiring decision based on an automated process without their consent.

They also have the right to appeal against any decisions made on that basis. If parts, or all, of your hiring process are automated, obtaining consent from your candidate to that making process is essential, together with transparency over the criteria applied in their selection or rejection from the application process.

If a decision is automated (i.e. in candidate screening) your candidates must be provided with an explanation for that decision. This can apply to candidates rejected during initial screening or following a video interview for example.



How an ATS can help

Complying with the GDPR will require a clear audit trail regarding your data management. Where data is stored in multiple locations, such as Excel, Outlook or Word – which is often seen in manual recruitment processes - compliance will be more complicated and time consuming.

Supporting your recruitment process with an ATS does not guarantee compliance with the new GDPR legislation. That responsibility lies within your business. It does, however, allow you to centralise all of your candidate data in one system, making it much simpler to monitor and evaluate compliance.

An ATS helps to ensure compliance with the GDPR in the following ways:

Candidate application forms

Most candidates today accept that automation is an integral part of recruitment processes but their consent to those processes is mandatory under the GDPR. Explicit consent must be obtained from every job applicant or candidate where data is gathered and stored in your ATS.

To comply with this ruling, provide a link to view your privacy policy within your candidate application form. That privacy policy must clearly state the length of the time the information will be held for before additional consent must be requested to retain that data for a further period.

This requirement also applies to individuals in your talent pool who register for automated job alerts or those who complete a registration of interest in future job opportunities or business updates from your company.

Schedule automated messages through your ATS to be sent to your candidates as the expiry date approaches to confirm their consent to their data being held on your system for a further specified period. Taking this step ensures that your company does not breach the requirements of the GDPR.

Your request for consent should also clarify how your candidate can object to your business retaining their data.

A further essential inclusion in your privacy statement should detail how candidates can object to the processing of their data. This must be provided at the beginning of the application process.

NB: A candidate's refusal to consent to non-essential use of their information must not be used as grounds to eliminate them from your hiring process. To accommodate a potential refusal, your ATS should allow you to adapt your forms and hiring process to reflect the level of consent provided.

Highlighting the use of 'killer' questions

Under the GDPR, candidates will need to be informed of any automated systems used during the application process. The use of killer questions or GNDs (Gross Negative Disqualifiers) is a key feature of a modern ATS which automatically rejects candidates based on specific criteria.

Examples of GNDs include whether the candidate has a valid driving licence or a specific qualification for a job. Employers and recruiters must obtain the applicant's consent to the use of this type of screening in advance.

Sharing candidate data

Employers and recruiters will still be permitted to forward a candidate's details via email to a colleague. If that information is downloaded and stored, however, this risks non-compliance.

An ATS which allows easy sharing of information on a dashboard which is accessible via a mobile device helps to resolve this issue. Hiring managers or interested parties can login to view information on a candidate without the need to download it.

Automated decision making

When decisions are made as a result of automated data assessments, your candidates must be able to request an explanation for - and a review of - this automated decision.

Your ATS can still make those decisions but to comply with the GDPR your privacy statement should highlight these processes and detail how to raise concerns or request information relating to candidate elimination and selection. In the context of automated background checks, clarity must be provided on why a candidate is being screened and how that screening will be carried out.

The nature of that screening (i.e. third party references, DBS checks) must be clarified together with details on who will be given access to the results.

Importing data from online recruitment channels

If your ATS currently allows your hiring team to create candidate records without their consent that will need to change. Recruiters who import candidate data from online recruitment channels such as social media and job boards must ensure that users understand their data may be shared.

To avoid non-compliance, your ATS should inform the candidate where you have obtained their details, request their consent to their details being held in your data base or provide details on how to remove that information.

Candidates already in your database must also provide consent to their information being held.

A GDPR summary action plan

- [ ] Review your existing procedures and recruitment process.
- [ ] Ask for consent from all of your candidates in the hiring process and explain why the data is necessary.
- [ ] Provide a clear privacy statement - be transparent.
- [ ] Take responsibility for your data cycle in the recruitment process.
- [ ] Comply with the right to be forgotten for rejected applicants and candidates who may not wish to remain in your talent pool.
- [ ] Allocate overall responsibility for an individual or individuals in your hiring team to ensure compliance.

Consider the following four questions:-

- If you receive a data access request from your candidate, how quickly would you be able to retrieve their information and respond?
- If a candidate asks you to update or rectify their personal data, this request must be met within one month. Can your business comply with this request?
- How familiar is your hiring team with the reasons for erasing or refusing to erase candidate data if requested? What policy do you have in place to deal with these types of requests?
- How ‘future proof’ is your recruitment process? Preparing for the GDPR will require a full audit to ensure compliance.

Questions for your ATS provider

Your ATS provider should be able to demonstrate how their system supports your recruitment process in complying with the GDPR, specifically in the following areas:

How effective are their data protection and cybersecurity measures?
This is essential to be confident that any potential breaches will be managed efficiently and effectively. Ask your ATS provider to demonstrate how they protect the data processed on your behalf.

Data breach procedures must be robust in order to comply with the GDPR legislation.

How will their ATS help your business to process requests for information from candidates?
With the removal of the administration fee for information requests, an increase in the number of requests is anticipated. Similarly, how will your ATS provider respond to the removal or updating of candidate records? All changes must be documented in the event of an audit.

Will candidates be able to access information via a self-service portal?
All candidates will have the right to request access to and change their personal data under the GDPR. Some ATS providers offer candidates a careers portal to complete application forms and participate in assessments such as psychometric tests and video interviews. An ATS which provides a self-service portal for candidates to update their own information builds candidate confidence in the accuracy of data held in your recruitment management system while minimising administration for HR and recruiters.

Does your ATS provider demonstrate that their technology will help your hiring process to comply with the GDPR?
It is essential for employers to provide evidence that all candidate data has been collected on a fair and lawful basis. Your ATS provider should be able to show how that information will be recorded in a way that complies with the GDPR.

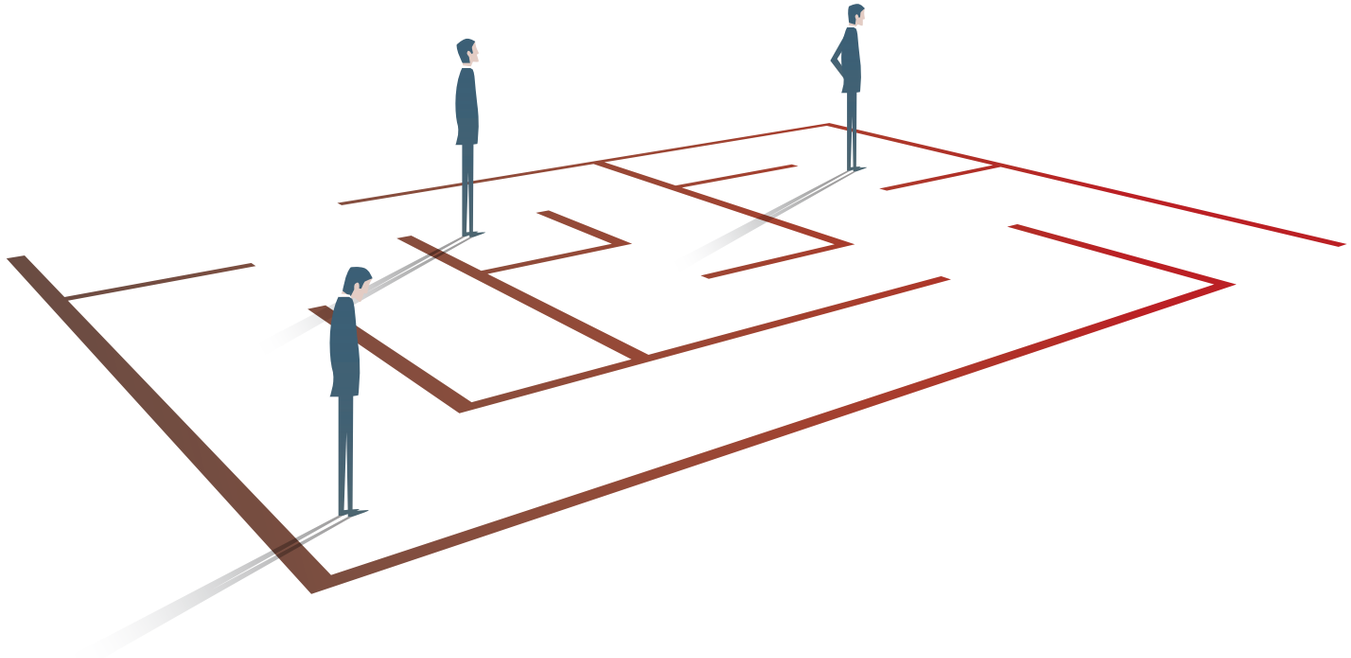
Is your business ready for the GDPR?

Ensuring your business is ready for the GDPR is a complex process but the potential for non-compliance can be offset with an efficient ATS which offers a centralised system for managing your data. The significant changes to candidate rights and data protection require a robust, transparent approach to ensure compliance. Supporting your hiring process with an ATS is essential to create a streamlined and responsive hiring process which complies with the new regulation.

Disclaimer

This eBook is a guide only and should not be relied upon or constituted as legal advice. To ensure your business is complying with the GDPR, please visit the resources below or take professional legal advice.

GDPR: EU Website • **ICO Guide to GDPR**



KALLIDUS

Look after your candidates

Speak with one of our experts to discover how our ATS integrates your fragmented recruitment processes into a single system, ensuring transparency in data management of your candidates and helping your business to **comply with the GDPR**.

+44 (0)1285 883911

info@kallidus.com

Find out more

kallidus.com

Twitter: @kallidus

Facebook: @kallidus

Linkedin: /company/kallidus

KALLIDUS