# TalentSpa Client Guide to GDPR

The General Data Protection Regulation is big news for the recruitment industry, changing how candidate data is handled. It is the revamped version of the EU data protection law.

From May 2018, the new changes will come into force, with hefty fines for non-compliance. But there's no need to panic just yet – we've covered everything you need to know to stay legal.

Here is our GDPR breakdown for recruiters:

**Holding Candidate data**

Recruiters must be able to prove that a candidate has consented to them holding their personal data. This means data that is currently on your system, as well as future data collected.

- ✓ Candidate data can't be held indefinitely, and consent is not indefinite.
- ✓ If you have provided a service or engaged in some way with a candidate, then this could be seen as implied consent, but best practice would be to confirm this through affirmative action to avoid any issues arising.
- ✓ Candidates must be notified of data collection, and consent to holding it within 30 days.
- ✓ Data held in a CRM system on candidates is also subject to the same rules. Please consult your CRM provider.

**How to gain consent**

You need 'affirmative action' to demonstrate a candidate's consent. Job board applications may gain consent as part of their process, but candidates applying via your own site will need to manually agree to consent. Where job boards provide details of consent to us we will aim to log them and make them available to you.

TalentSpa and many of the larger job boards have advanced programmes to help monitor and log consent. In the case of smaller niche boards, where we may be unsure whether consent has been properly granted, we're pursuing ways to reinforces this.

- ✓ Consent could be a simple tick box with a statement along the lines of 'I acknowledge and give permission for my data to be held by (Business name) in accordance with the General Data Protection Regulation'.
- ✓ Application pages hosted by TalentSpa will be updated to include a consent tick box
- ✓ Tick boxes can no longer be pre-checked. Similarly, emails won't be able to assume consent by saying 'Please click on the link below if you want us to continue to hold your data. If we do not hear from you we will assume it is OK to retain it'. Instead, they will have to say something like 'Please click on the link below if you want us to continue to hold your data. If we do not hear from you within 30 days your details will be removed.

**What are we doing?**

1. We're amending the system so you can specify how long you wish to retain candidate data for. There have been conflicting opinions on the duration data should be stored without re-confirming consent, so each client will be able to set their own duration (we will advise once we have clarity on what is expected)
2. The system will be updated to specifically log consent (date and time). We'll be introducing a 'candidate retention period' parameter, after which point consent will automatically need to be re-obtained.
3. If consent is not granted then candidate data will be removed from Talent Pools and will no longer be available via the candidate and vacancy menus. Statistical data will be retained.
4. Our intentions are to record details of consent by time, date, source and type (verbal/written). We're also exploring a range of technical options and product enhancements to assist with the recording of consent (We'll provide updates on this before May 2018).

## Checklist for requesting consent from candidates

When you initially contact a candidate or are looking to regain consent to hold their data, you need to be clear about what the data is, why it's being held, and outline their legal rights.
Things to include in your consent request should be;

- ✓ Your contact details
- ✓ Purpose of processing data
- ✓ Categories of personal data held
- ✓ Who the recipient might be
- ✓ If its to be transferred outside the EU, how it is protected
- ✓ Origin of personal data
- ✓ Period to be stored or criteria used to define storage period
- ✓ The logic of any automated processing
- ✓ How a candidate can exercise their rights
- ✓ The right to withdraw
- ✓ The right to complain to a regulator

## Accessing Candidate Data

Candidates have the right to request access to any data held about them. You need to create a place to log these requests. These requests can be verbal, electronic or hardcopy. Candidates have the right to request changes to their data, to rectify mistakes and to have the data erased (including any notes and comments about a candidate).

If data has come from a source other than a person, candidates are entitled to know where it originated from.

Requests to access, amend or erase data should be provided as a free service for candidates, to be provided 'without undue delay and at the latest within one month of receipt of the request'.

**What are we doing?**

1. We'll create a function for you to download all candidate related data (including CVs, application forms, notes and comments). It is your responsibility to then forward this to the candidate.
2. Our system will log the event for audit purposes. There is no fixed format for this data and therefore we'll be making it available in Excel, PDF, Doc and similar formats.

It is worth highlighting that this access right includes "all data" so you may like to look at historical data for recruiter comments.

Right to be forgotten – Candidates may request at any time to be forgotten

**What are we doing?**

1. A function will be created so that a candidate's data and all associated records are removed.
2. The candidate will be notified of this. An audit record will be created to record the event.
3. Where a candidate is automatically removed (due to consent not being obtained), we are not intending to notify them of their removal.

**Automated Processing**

There must be some human intervention when making decisions about candidates. Decisions about candidates based purely on automated processing are not permitted.

Parsing software, which searches CVs and matches them to a job role, should be OK provided the decision to interview and hire candidates is made by a human being.

**TOP TIP** – Audit your data to ensure everything you hold is compliant. Keep a record of:

- ✓ What data you have
- ✓ Where it is kept
- ✓ Who has access to it
- ✓ How it is stored

**Our joint legal obligations**

In the past, responsibility for complying with data protection rules has fallen on recruiters (the data controllers). But under the new legislation, TalentSpa (the data processors) are equally liable.

We take out information security very seriously, so we're investing substantial time and resources to ensure we remain legal, and that both our services and clients comply. We will be making system changes and reporting so you can show that you're compliant regarding data held in TalentSpa.

Our role is to supply you with the tools you need to ensure your business operates within the new rules. But we can only go so far! Outside of TalentSpa you need to be able to demonstrate that any data downloaded is secure. This includes everything on your server such as spreadsheets, outlook/mail and external folders We're already logging all download events such as CVs or Excel reports.

We currently have audit trails for all candidate actions that happen within TalentSpa and will be adding additional parameters such as Data Retention Period and consent dates to aid compliance.
TalentSpa must be able to demonstrate that information security is at the forefront of our developmental decisions. As such we are currently obtaining ISO27001 accreditation.

**Additional measures we will be taking:**

- ✓ We now run annual penetration tests, results will be made available upon request
- ✓ We will only be using HTTPS wherever possible
- ✓ Intrusion Detection system
- ✓ Data access control
- ✓ US privacy shield
- ✓ Staff Background checks
- ✓ Annual audits

## Checklist for data security of your business

The GDPR is not just about your relationship with TalentSpa, it also concerns the data security of your business as a whole. To access the wider security of your business, you should be considering the following questions:

- ✓ Has every leaver had their access to all systems (and your office) revoked?
- ✓ Do you have a data retention policy?
- ✓ Do you know where your data goes?
- ✓ Are you registered with the ICO?
- ✓ Are your staff regularly trained on data security?
- ✓ How secret/strong/rotated are your passwords?
- ✓ Do you have a Privacy Impact Assessment?
- ✓ How many people have access to your systems?
- ✓ How are you protecting your local systems?

## Contractual Obligations

As a data processor we have a comprehensive programme underway to ensure we are compliant with the new legislation, whilst assisting our clients with their compliance obligations. We do not recommend that you rely solely on TalentSpa to help you achieve compliance and if you are in any doubt seek professional advice in this area.

**Conclusion**

We're working hard to ensure our services meet the new regulations, and we're implementing some important system updates to make this possible. This increased functionality will make compliance easier for clients using our services, focussing on the three core areas of candidate consent, access to data, and right to be forgotten.

If you would like to know more about how our services will be updated to accommodate for the new GDPR rules, get in touch with us.