GDPR for the
Recruitment Sector
Your Questions Answered

Do we need to contact all individuals that we currently have on our database for consent?

To be compliant with the General Data Protection Regulation (GDPR) you should never contact anyone you do not have consent from.

We advise that you first go through your database and do a full “audit” of who you have and have not got ‘proof’ of consent from. If you have recorded and can demonstrate when and where an individual gave consent, you are safe. However, if you have not, then you need to review your data.

You can use this as an opportunity to review the details you currently hold and whether you need them. For example, if someone has never opened one of your emails or has not interacted with you, for example for three or more years, you need to ask yourself whether you really need to keep their details.

In some instances, businesses are sending out mass emails to get their database to opt-in. However, this could be deemed as against the regulations if you do not already have consent, or it could shrink your database because no one might contact you to opt-in. We advise you to direct those who you do not have consent from to an opt-in form on your website. This way you can obtain consent and “proof” to contact them again.

At this point it is important to remember that you cannot contact anyone who has already opted out. If you are in any doubt about contacting someone, err on the side of caution and do not contact them.

Can we put a message on our phone system before we answer to state: “the caller is complying with the GDPR”?

We do not believe that this is necessary. However, this is something you need to consider if you are recording calls where personal data/information will form part of the conversation/call. In these instances, any personal data you collect, which is subsequently recorded on your systems, must be protected, safeguards should be put in place to keep it secure and you need to make the contact aware that their information is being stored.

What would be the best way to deal with erasure requests if the majority of your candidate data is shared with third parties. How would you be able to confirm - outside of contractual agreements - that the data has been deleted?

If you collected the data initially, you are the ‘controller’ and subsequently responsible for that data. The onus is on you.

Firstly, after 25 May 2018 it is best practice to ensure that the third parties you share data with are compliant with the GDPR. This will mean that should you ever need to erase data, they will already have processes in place to do so.

Once you are notified by a candidate to erase their data, you need to ensure it is deleted from all your systems (front end and back end). You then need to notify the third parties you use to instruct them to delete the applicable data. You should at this point look to get in writing from the third party that they have deleted the data.

We can see that after 25 May 2018, a key selling point for firms and software providers will be that they are compliant with the GDPR.
Within our company, each recruiter has their own database of candidates. Is there a way to keep candidate details in case they contact the company in the future so that the company can keep track of candidate “ownership” within the recruitment team? We already have an opt-out feature where they no longer get emails from us, but we retain their records.

In this case, I think you need to determine what details you need to keep on record for this. If an individual is purely on your database for future reference, do you really need to keep all of their CV details or would just a name and email be suffice. Once you have done this you can mitigate your risk by deleting any unnecessary information.

I would also advise that when you engage with a candidate you have a clause in your contract to say that you will keep their contact details for future reference. Just make sure that if they ask to be ‘forgotten’ you do delete all of their details.

If an individual sends you their CV by email, i.e. in response to a job advert, is that consent or do you need to email them back something that then asks consent?

If someone sends you a CV, essentially, they are consenting for you to contact them. However, it is best practice to ask them to consent to further communications, or at this point create an engagement agreement with them. This will ensure you are covered now and in the future. This engagement agreement can be simple - “I’ve received your CV, can you just confirm that you are happy for me to use and share your CV with third parties to find you a job.”

Do we need written consent to hold or process candidate data, or can they click an opt-in feature on our website/link or email etc.?

An opt-in form from the website or an email is sufficient proof that you can contact a candidate again. Just make sure you keep this as a record so that you can demonstrate you have consent form an individual should you ever need it.

What do we do with regards to company mobile phones, which have telephone numbers and candidate emails?

If you have a candidate's personal data on a mobile phone, this is covered by the GDPR and you will need to ensure safeguards and precautions are in place to protect that individual’s data. You are responsible for it and need to demonstrate that you have put processes in place to protect it.

The GDPR states that a ‘data controller is not obliged to comply with an access request if that would result in disclosing data about another individual, unless that other individual has consented to the disclosure.’

In regard to references. Even if we were to redact identifying particulars and share the reference with the individual it would most likely still be possible to identify the other party or individual who supplied the reference (as their name will have been given to us by the data subject themselves). In such a case, I presume this would be considered information about another individual (even though the data in question is about the data subject) and we would not be able to disclose the reference without consent from all parties?

We agree that the reference is in confidence and therefore cannot be shared without consent. We are unsure though why you would need to share a reference with a candidate. If you are required to do so, then the best practice would be to get consent from the individual providing the reference.

However, this does not seem like a GDPR issue but more an employment law issue with regards to sharing references.

Can recruitment agencies access references, without consent, from the referee?

In most instances, you will get referee contact details from the candidate themselves. If a candidate has given you the referee details you can assume that the candidate has spoken to the referee and got consent for you to contact them. If you have something on file, e.g. email from the candidate to say that you can contact the referees to obtain a reference, you have been given consent and are covered.
Just a question in terms of receiving updated consent from individuals held on your database. If the database you are using does not keep record of whether your communications have been interacted with by the individual, particularly if the individual in question is a historic record (e.g. over ten years on the database), would you have any legal basis to contact them?

Firstly, in the case of having records for over ten years, you need to decide if it is reasonable for you to still have this information if you have not interacted with them in that time.

If you have no record of consent, you cannot contact someone. You need to make sure you have ‘proof’ that you can contact someone, e.g. an email or a website opt-in form. It is best practice that where you do not have this proof, you seek to obtain it or no longer contact that individual.

What about passport details or utility bills of candidates that clients ask us to check as due diligence and proof of address etc.? Can we keep these on file?

These checks are part of the recruitment process; therefore, it is legitimate for you to capture this information. However, once the candidate has been placed, it is probably not appropriate for you to keep this information long-term. Maybe set up a reasonable amount of time, say six months to a year, after a candidate is placed and delete this information. Showing you have thought about these different scenarios and have processes in place will ensure you are covered.

What are the rules for sharing CV’s with Rig Managers not based in the EU?

Firstly, GDPR is an EU initiative so if you are a firm in the EU or are sharing information with businesses based in the EU, you need to ensure you are all complying with the GDPR. However, once you start sending information outside of the EU you need to look at the contractual terms that you have in place with that end user or company.

Despite the third party being outside of the EU, you are based in the EU, which means any contracts you have in place must be compliant with the GDPR. Regardless of whether you are sharing data with people inside or outside of the EU you should keep to the GDPR terms as you are the ‘controller’ of the data and therefore responsible should any breaches happen. Going forward, we can see that those businesses outside of the EU will have to make themselves compliant with the GDPR in order to win business and work with EU companies.

We must admit thought that this is a slightly grey area; going forward it is recommended that before you enter these arrangements you call the ICO helpline (0303 123 1113) and get their advice.

How long can we store an applicant’s CV?

The GDPR does not set out any specific minimum or maximum periods for retaining personal data. It says that, “Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.” Therefore, you need to look at what you are using the data for and determine what the necessary time for you to keep the data is. For example, if you placed a candidate five years ago and have not been in touch since, is it necessary for you to keep their data?

One solution is to decide on the key information you need from a candidate and delete the other information, i.e. keep their name and email, but delete their CV. This will limit your risk as you are not keeping unnecessary data.

How long can we store interview feedback/ notes for?

You need to decide as a firm whether this information is necessary to be kept for a prolonged amount of time. We recommend that once you have placed a candidate in a role you review what information you hold about them and decide how long is necessary for you to hold that information.

This also depends on the candidate type. For example, if you place contractors, you know that they may need another position in six months’ time and therefore it is necessary for you to store the feedback, but if you placed a client two years ago and they are not looking to move jobs, you need to ask whether you still need their information on your systems. If you have a compelling reason to hold data and have proof of that, you will be fine. You just need to demonstrate you have processes in place and clear time-frames for such information.
With whom can we share applicants’ details internally?

This is ultimately determined by your ‘contract’ with your candidate. If you have an agreement in place that you are looking for a job for a candidate, you will have a legitimate reason to share their details internally. Once a candidate has communicated that they agree for you to find a job or contact them, you can, within reason, do anything necessary with their data to find them a job. Just make sure you have that initial consent from the candidate.

If I add a candidate’s details (CV/profile and contact details) to my own internal database, either from LinkedIn or a CV Library, with a view to making contact so they are aware of me should they be looking now or in the future for opportunities. Is this permitted under the new GDPR rules? I.e. Do I need to have their permission from the outset for me to hold their details even if they are already out there in the public domain?

To ensure you are fully covered, you should get consent from the candidate or at least make sure they are aware you are storing their details on your database. It could be argued that there is no legitimate reason for you to hold the candidate details on your database if the information is already in the public domain. I.e. you can obtain them when you want. It is always best practice to ask the candidate first and check that they are happy for you to store and use their personal data.

We are a company that buys contact databases from companies likes of Hoovers, Zoominfo etc. We use this contact information to send email campaigns to prospects around the world (B2B). At this point in time, we do not know if our data supplier has acquired consent from the individuals on the lists we purchase. So, we just put in an ‘Unsubscribe’ button at the bottom of our emails.

Keeping in mind the GDPR requirement, would the above method be good enough to comply to the regulation? Or do we need to ensure that there is consent first before sending out the email campaigns?

The GDPR effects personal data and not B2B so if you email to a B2B email address then you should be covered subject to giving the recipient the option to opt-out.

However, if it is B2C data. It is best to ask the company you purchased the database from if they have consent. You then need to keep a record of all the individuals who have given consent (when they gave and the format they gave you). If you do not have this consent, after 25 May 2018 you should not be contacting them.

Please call the ICO helpline for further advice on this.

For GDPR support and advice contact suda.ratnam@raffingers.co.uk
or
Call the ICO helpline on 0303 123 1113

Disclaimer

• The information contained in this document is for general information purposes only and should not be construed as giving the ground for any action or omission in connection with the above material.
• This document should not be construed as professional advice.
• The examples given in this presentation are described with a level of detail that does not provide for their implementation without additional comprehensive review with due regard to specific relevant facts and circumstances.
• The application of laws may vary depending on particular circumstances.
• Raffingers LLP does not assume liability for any damage that may be caused to anyone as a result of any action (or omission) on the basis of the information contained herein.