



GDPR Questionnaire

If you are a recruitment agency, you need to make sure that you show transparency and accountability in regard to protection of all personal data of your clients and candidates. The questions below will help you to prepare for the new regulations and your recruitment agency, so you will be able to demonstrate GDPR compliance.

General questions:

- Do you have an internal audit of your data to identify what data do you hold and why?
- Are you using the right channel to contact individuals who gave consent for it?
- Do you have procedures in place not to contact unsubscribes?
- Is everyone in your agency aware of the GDPR?
- Do you inform your candidates about their rights and consent to use their data?
- Did you appoint a Data Protection Officer DPO?
- Do you take additional precautions to make sure your data is protected?
- Do you have an updated privacy policy?

Organisation:

- Do you have a senior management team responsible for IT security?
- Do you need to transfer personal data abroad?
- Is the transfer providing adequate protection for the rights and freedoms of data subjects?
- Are you processing payment details for your company or customers?
- Has your company been certified PCI compliant?
- Does your Privacy Policy inform users about their rights, how you collect and process their data?
- Are there any Information Security weaknesses you are aware of?

Authentication:

- Do you use user IDs and passwords to authenticate logons?
- Do you supply one user account per member of staff that uses your system?
- Do you enforce minimum password standards?
- Is the password database hashed or encrypted?

Access control:

- Are administrative privileges controlled and only allocated as specifically required?
- Is access provided on a strict needs-only basis?
- Is a list of users maintained?
- Are inactive users removed from the system?
- Do you display a notice prior to logon to indicate that your system must only be used by authorised personnel?

Data Encryption:

- Do you use encryption methods to protect data in transit and storage?
- Do you have a defined data retention and deletion policy?
- Is wireless networking in use?
- Do you use network encryption and access control methods?

Computer Protection:

- Are all systems protected by Anti-Virus? If yes do you update them regularly?
- Are you using tools to monitor security and access?
- Is computer hardware (servers, workstations, routers, etc.) protected against physical access?
- Is computer hardware protected against fire, flood or burglary?
- Is data protected against loss or corruption by regular backups being taken and stored separately?



**Need help getting
your website
GDPR compliant?**

