BioTalent Ltd GDPR Q&A for Clients

Question	Response
What personal data do you process on behalf of THE BUSINESS?	Any data which relates to an identifiable person. (Candidate). Name, address, mobile, email, NI, passport, driving license, career history etc.
For what purpose do you process this personal data? *"Purpose" is the specific reason why you are processing the data.*	Data is collected for specific, legitimate and explicit purposes of recruitment in order to help our clients find the right candidates for active and at times non active but for the right candidate positions within the Hiring company's business. As well as aiding candidates with their search for a new position either in the Contract Market or the Permanent market.
What are the risks to data subjects' rights and freedoms if the personal data is destroyed, lost, altered, disclosed without authority, or accessed without authority. *Consider likelihood and severity.*	We believe the risks are minimal in so far as the information we obtain is contained solely on our database and is not shares with any outside third parties, except with clients who a candidate's skill set may be suitable for. In the event lost, altered etc.. The likelihood is the candidate could report us to ICO with fines of up 4% of our turnover. There are also potential compensation claims that can be made by the data subject. Reputational damage – ICO will name non-compliant organisations affecting our reputation in the industry with clients/candidates. Although the risks are high in relation to penalties, this is UK wide on all recruitment firms but we believe the risks are low in relation to your suggestions. Worst case – ICO can stop us processing personal data.
What technical and organisational security measures do you have in place to ensure a level of security appropriate to the risk. Consider: 1. Pseudonymisation and encryption 2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; 3. The ability to restore the availability and access to the personal data in a timely	1 Data Backups are stored off site with a strong encryption. Files on the server are not currently encrypted. 2 Files can be restricted to users or groups that have a need to access if required. 3 The server is backed up as an entire image and can be restored quickly in the event of a physical failure or in the event of a disaster. Emails are not backup up beyond 14 days.

manner in the event of physical or technical incident; 4. The process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	4 Data Backups are tested on a weekly basis. 5 The Server is monitored 24/7 for performance / System errors to help prevent system failures. 6 IT equipment / Server software & Security updates are managed / updated centrally.
What provisions do you have in place to either delete or return the personal data once the service comes to an end?	1. Consent 2. Legitimate interests of controller 3. Performance of contract 4. Compliance with legal obligation 5. Protect vital interests of data subject 6. Perform task in public interest This is placed only when requested by the Contractor or perm placement. At the point of request we will task our ops team to contact the data subject, discuss the deletion or return of records and remove accordingly. Otherwise it is our intention to keep the candidates details on the system, as this coincides with our "legitimate business interests" but is also in the interest of the data subject who may be seeking a new position on a sporadic basis.
What provisions/training do you have in place to ensure that your employees process the personal data in accordance with THE BUSINESS's instructions?	We are engaged with our commercial and operations team and have scheduled training sessions in January and February of 2018. The directors have already been involved in the preparation and consulting side and have a slide show for presentation to the business already prepared.
What process do you have in place to identify personal data breaches and notify THE BUSINESS without undue delay?	Clear and transparent notice of how and why we will process their data and for what purpose (currently being drafted) to include the below matters. • Where we obtain CV from job-board? • must give candidate our privacy notice within 1 month, or at time of first communication, whichever is earlier • How do we give candidates notice of the policy? • Email auto-response to candidates who apply via job-board or respond to mailed opportunity? • Pop up box when they apply through our website? • Include link in email signatures? • Display on website

Do you understand the GDPR requirements in detail and are you satisfied that you are aware of the impact these will have on your business?	Absolutely as defined in risks above.
Do you have dedicated personnel/project teams working on GDPR compliance to ensure you are GDPR ready before 25th May 2018?	Yes our commercial and operations teams are in advanced preparation for our business to be as compliant as one can be.
Have you completed a gap analysis and do you understand the activity required in order to be GDPR compliant?	Yes. However it is also our intention to engage with external experts on the matter who will provide an audit of our preparation in order we are compliant and can run the processes out to the business.
Do you anticipate full GDPR compliance by 25th May 2018 or before?	Yes.
Has your work to date identified any changes that will be required to our relationship as a result of GDPR? If yes, please provide high level details	None whatsoever.
Is there any further information you can share with us about your GDPR preparedness at this time?	We have attached a copy of our commercial team' business GDPR presentation.
Is there anything you need to know from us?	Not at present thanks.