

## GDPR – Assessors/Partners

GDPR came into force on 25<sup>th</sup> May 2018 and is the first major update to data protection legislation for a number of years. A number of the changes have been made to bring the legislation up to date with the type of data processing that can now take place, such as how Facebook suddenly knows that you are interested in Bungy Jumping immediately after you have been looking at other websites, or using your online behaviours to target marketing to you or process your likes/dislikes/demographic info. Also, the extent of data that is held has increased significantly and there is now much more awareness of identity fraud. Just as our house or car is our own property, so is our personal data and it needs protecting.

There is a lot of information being circulated about GDPR (there are also some very expensive courses and consultancy services being offered!). The ICO have produced some resources, using the second link will take you through a self-assessment that we encourage you all to complete and act upon:

<https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf>

<https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/>

### Key Terms in the Legislation:

The GDPR applies to ‘controllers’ **and** ‘processors’.

A controller determines the purposes and means of processing personal data.

A processor is responsible for processing personal data on behalf of a controller.

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

The GDPR refers to sensitive personal data as “special categories of personal data”. The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and

deliberate causes. It also means that a breach is more than just about losing personal data.

For your work with Assessment Services you will be a 'Data Processor', whilst Assessment Services will be the 'Data Controller'; it is unlikely you (or Assessment Services) will be processing sensitive personal data.

### **What personal data will you be processing?**

Key contacts: through most of your communication with organisations, you will be corresponding with your key contact. This information is held on Net Suite, and you need to ensure if there is a change in key contact that this information is updated to ensure correspondence is directed to the appropriate person.

Planning/interview information: Often customers will send you the personal details of people you will be interviewing, e.g. names, telephone numbers etc. You will need this information to plan the assessment and/or undertake the scheduled interviews. If information such as telephone numbers, clients' names etc. are provided to you once you are on-site, then once you have used the information leave the documents including this information with the customer at the end of the assessment. If the customer has sent you this information electronically, you must delete it from your system within 4 weeks of going on site. As per your assessor agreement, all interview notes should be kept for 12 months and then confidentially destroyed e.g. shredded.

Onsite information: Customers will provide you with a range of information whilst you are on site. Publicly available information e.g. Student Handbooks, marketing materials may be kept. However, any confidential information must remain with the customer; if you feel you need the information to complete the assessment report, you must gain the permission of the customer and confirm that you will destroy it confidentially agreeing a timescale.

### **Do I need to be registered with the ICO?**

As an assessor/partner you will need to determine if you need to register with the ICO as it will depend on the nature of all of the work you undertake. There is a questionnaire produced by the ICO to help you decide:

<https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf>

### **What if things go wrong?**

Tell us! Data breaches need to be considered and we may need to self-report to the ICO.

When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we must notify the ICO; if it's unlikely then we don't have to report it.

However, if we decide we don't need to report the breach, we need to be able to justify this decision, and therefore we will document it.

**Whose responsibility?**

All of us – both as 'controllers' and 'processors' of data, we all have responsibilities to safeguard personal information. As a subcontractor and being self-employed it is also your obligation to ensure GDPR is addressed.