APSCo Update on Legal & Compliance Issues

May 2017

Topic: General Data Protection Regulations (GDPR) – Enhanced Rights for Individuals and APSCo's Data Questionnaire

The new EU Data Protection Directive, known as the GDPR will come into force on 25th May 2018, as is likely new e-privacy regulations. Despite the fact these are both EU derived the UK Information Commissioner's Office (ICO) have made it clear that post Brexit these laws will remain.

We will still need to share data with the EU, plus the ICO recognises the need to bring the law up to date and future proof it to take into account the myriad ways in which personal data is used and accessed online.

This is a business critical area with multiple touch points for recruiters. Put simply you are in the business of using the personal data of clients and candidates to make introductions and arrange placements. You may also employ large workforces about whom you hold and process considerable amounts of personal data.

Under the GDPR an individuals' rights are much stronger and potentially more disruptive. Your systems and processes will need to handle demands from your employees and business contacts with the scope for a significant nuisance factor and of course the enhanced fines for breach of up to €20M or 4% of global turnover whichever is greater. There will be generally strict legal liability for data breaches.

Individuals have the right to:

- transparency of use of their data (to be kept informed)
- access their data – within a maximum of a month of request (a Subject Access Request)
- correct their data (you must also tell third parties if you have disclosed inaccurate data to them)
- have their data deleted where there is no "compelling" reason to process it (the right to be forgotten)
- block or suppress processing of their data
- obtain and reuse their personal data across different services (data portability)
- object to processing based on "legitimate interests" or direct marketing (including profiling)

You will have 72 hours to notify the ICO in the event of a personal data breach, and any delay in doing so must be explained (Article 33)

Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons the individual must be told of the data breach without delay.

ICO are regularly publishing guidance and there is an overview (which is maintained) https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

The GDPR requires sound data governance and must be a key focus of your group strategy. Up to

The Association of Professional Staffing Companies Ltd
101 Borough High Street, London SE1 1NL
Tel: 08458 997388 Fax: 08458 997389
Email: info@apsco.org Web: www.apsco.org

now data protection may have been a side issue but "privacy by design" and "privacy impact assessments" are legal requirements and making privacy key to your business will enable compliance.

> The GDPR applies to 'controllers' and 'processors'. The definitions are broadly the same as under the Data Protection Act (DPA) – i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf. The controller and processor may be the same legal entity or person. Processors maintain records of personal data and processing activities and have significantly more legal liability if they are responsible for a breach under the GDPR.
>
> However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

APSCo will be focusing on the following to support our membership:

1. Understanding what personal data you hold, where it is and what you do with it. This is generally the starting point for any work on data. You may need expert assistance, e.g. from our legal affiliates, on this process. However, as a starting point we have prepared a **Data Questionnaire** – you may wish to go into considerable detail or use it as a starting point to identify your key risk areas.

2. Compliant collection and processing of data. Recruiters have been able to rely on implied consent to process data. This is not possible under the GDPR. Recruiters need to consider ways of obtaining express consent and other legitimate reasons for holding and processing data. Individuals have far greater rights under the GDPR.

3. Retention and management of data. Many recruiters do not have a retention of data policy or formal processes for managing data, including deletion of data, which they adhere to. This is necessary under the GDPR as there are more individual rights such as the right to be forgotten and portability of data.

4. Data Security Recruiters are aware of the need to have secure databases and IT systems but security processes will need to be robust given the potential fines that can be levied by the ICO and the ever increasing cyber threat.

5. Marketing and Keeping in Touch with Candidates and Clients Recruiters will need to reconsider their marketing strategies in light of GDPR and in all likelihood treat far more of their day to day communications as marketing. This is an area where APSCo hope we can agree best practice with our membership.

The Association of Professional Staffing Companies Ltd
101 Borough High Street, London SE1 1NL
Tel: 08458 997388 Fax: 08458 997389
Email: info@apsco.org Web: www.apsco.org

6. Appointment of a Data Protection Officer All recruitment firms need a key individual responsible for data compliance. Non-public authority businesses only have a legal duty to appoint a DPO under the GDPR if they carry out large scale processing of special categories of data (akin to "sensitive data") or systematically monitor individuals (e.g. online behaviour tracking).

7. Incorporating "Privacy by Design" and "Privacy Impact Assessments" into your processes and operations.

APSCo Strategy for Engagement on GDPR

Presentations and guidance by our affiliates - at APSCo meetings and forums and circulation of guidance and information published by affiliates to assist with implementation.

APSCo Working Group on implementation – to discuss and share best practice. It will also be used as group to consider whether it is appropriate and practical for APSCo to formulate a GDPR Code of Practice to be adhered to by its members and affiliates.

Toolbox documents on our website – these will be useful as a starting point and a guide for the work you need to undertake over the coming months. Our first document is the Data Questionnaire.

Updates from us, our members and our affiliates via the APSCo Linked In members group

Regularly updated FAQs and Guidance on the GDPR on our website.

Actions to take now

- Establish an internal GDPR project team – this should include sales representatives and report to your board.

- Complete a data audit using our questionnaire or obtaining specialist advice. You have to understand what data you hold, where it is and what you do with it. This will highlight key weaknesses which could be legal documentation, systems, training, HR or marketing. Following this audit your project team should be in a position to establish priorities for your business.

- Consider what external support you may need to comply – whether that is support on managing data, system adaptations, legal support or marketing expertise.

We are very keen to hear from affiliates who are able to offer services to our members to help them comply with the GDPR – we are also keen for affiliates to contribute guidance and updates

The Association of Professional Staffing Companies Ltd
101 Borough High Street, London SE1 1NL
Tel: 08458 997388 Fax: 08458 997389
Email: info@apsco.org Web: www.apsco.org

which we can circulate to members and add to the GDPR Toolbox on our website. Please contact Tania.bowers@apsco.org

The Association of Professional Staffing Companies Ltd
101 Borough High Street, London SE1 1NL
Tel: 08458 997388 Fax: 08458 997389
Email: info@apsco.org Web: www.apsco.org