APSCo Briefing on
Legal & Compliance Issues

May 2016

Topic: Impact of the proposed EU General Data Protection Regulations on Members

Introduction

The new EU Data Protection Directive, known as the GDPR was approved on 4th May 2016 and member states, including the UK now have until 25th May 2018 to comply. If the UK votes to leave the EU in the May 2016 referendum then implementation of the GDPR may be subject to change.

This is a complex 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.

Personal data broadly speaking is information held about a living individual.

We will be producing a series of information pieces and guides over the coming months and years, in partnership with our legal affiliates, to assist you with understanding and responding to the challenges of the new law.

Below is a summary of some of the key issues affecting your businesses and how the landscape will change in 2018.

- **Data Protection Registrations**

Current Position

Register in the UK as a data controller and processor.

Review registration requirements of all countries in which you operate and register in each individual country as required.

Future Position

All companies will have to retain information on their processing activities. This may replace registration.

You will only need to register in one country in the EU "the lead country" of the group of companies.

There may be a requirement for companies to appoint a Data Protection Officer in certain cases (for example public authorities or organisations whose activities involve regular and systematic monitoring of data subjects on a large scale).

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

- **Consent**

Current Position

Recruiters largely rely on the concept of "implied consent" to process individual's data, whether candidate or client, both here and internationally. This can be obtained by a candidate registering for a role, working through an online application process or by a client receiving "services" whether through a placement or simply emails informing them of potential candidates. Recruiters retain the data, possibly indefinitely, for their marketing purposes. Many may inadvertently breach non UK country specific laws by doing so for example those in Holland and Australia. Many countries have far stricter SPAM (unsolicited marketing) laws than the UK.

Future Position

Express consent by opt in or other suitable mechanism will be required to process data. It cannot be assumed that consent is given for wider purposes nor that it is given to retain data indefinitely. This will result in a more level playing field globally. However, recruiters will face difficulties maintaining their existing business processes and marketing practices. They will need to think of innovative means of collecting consent and make their services more attractive and urgent to their customers. This will include providing newsletters and "add on services" such as training as a means of "keeping in touch".

- **Penalties and Fines**

Current Position

In the UK the maximum fine the Data Protection Authority can impose is £500,000. In addition, the DPA is primarily concerned with large scale data breaches and has a light touch approach to general compliance. In other countries recruiters already face challenges when dealing with data complaints and may face legal action, investigations by regulatory authorities and fines.

Future Position

Fines will increase significantly to up to Euro 20M or 4% of global turnover whichever is greater. However, it is still likely that individual countries will have differing approaches to data breaches and the severity of enforcement.

There will be strict liability for reporting data breaches. It is possible that there will be a statutory duty to report, however minor the breach.

- **Approaches to Processing Data**

Current Position

In order in order to use information compliantly under the current Data Protection Directive and therefore the Data Protection Act, it should be:

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

- used fairly and lawfully.
- used for limited, specifically stated purposes.
- used in a way that is adequate, relevant and not excessive.
- accurate.
- kept for no longer than is absolutely necessary.
- handled according to people's data protection rights.
- kept safe and secure.

Future Position

The principles set out above remain.

Privacy by Design – incorporating data protection compliance as a deliverable into all of your activities e.g. CRM system design, compliance targets, internal projects.

Risk based approach – assessing data risk throughout all of your activities and taking appropriate mitigation steps.

The Right to be Forgotten/the Right to Object to Profiling – Individuals will have greater rights to control how their data is processed and to view their data.

The Right to Data Portability. Date subjects will have "a new right to obtain a copy of their personal data from the data controller in a commonly used format."

Note the law has already changed in this area as ECJ decisions provide individuals with enhanced rights to be forgotten. For example, this has altered Google's approach to delivering search results.

- **International Transfer of Data – intra group and to external parties**

Current Position

It is time consuming, complex and expensive to be compliant under current laws. Binding corporate rules between group companies are required but these may need registering with in-country Data Protection Authorities. It is difficult to export data compliantly outside of the EEA.

Many organisations rely on the US Safe Harbor arrangement but this is no longer reliable since an ECJ decision in October 2015 and has been replaced by the Privacy Shield Proposals announced in February 2016.

Future Position

It is difficult to anticipate what the future position will be. One advantage is likely to be the "one stop shop" whereby a group can communicate with one country's authority in respect of its activities in the EU.

- **Some Actions to be considered**

Consider "consent to process" – how do you use personal data now and anticipate using it in the

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

future.

Talk to your suppliers about their data compliance and in particular your system suppliers about how they intend to ensure their systems are compliant with the new GDPR or how they could assist with their customers' compliance.

Review your contracts with your suppliers to ensure there is a clause requiring compliance with UK and EU data protection and privacy law.

Think about the resources to prepare for change. Identify who takes overall responsibility. Ensure that they have the time and support to plan for the reforms.

Review privacy notices and other fair-processing information given to employees clients and candidates. Consider what additional information will need to be included.

Review contracts of employment, handbooks and policies to see whether and how they deal with data protection (and in particular, whether contractual "consent" is sought).

Establish a policy (with a timeline) for handling data breaches. Obtain a full picture of exposure to potential data breaches by ensuring that breaches and loss are reported to whoever is responsible.

Train staff on data protection responsibilities and how they affect their job.

Develop and implement a policy on retention and storage of data, including emails.

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