

## The EU General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. The new directive will come into force in **25 May 2018**.

Naturally many of our customers are asking about Vacancy Filler's compliance with GDPR and are taking a closer interest in how we protect candidates' data.

Processing candidate data has been our core business since the company's inception in 2009. Our position is that we do not see any significant changes to the way we manage our customers and their candidate data except for the fact that the lines between Data Controller and Data Processor are more blurred meaning that there is a joint responsibility between the customer and supplier and also that fines for breaches are considerably higher. Consequently, customers are carrying out greater due diligence.

Below is our data policy statement:

- Unlike some of our competitors, we do not act like a job agency and pass on candidate details to other customers. Every candidate processed on behalf of our customers remain the customers' candidate
- We will work with each customer to ensure that there is an adequate consent statement when a candidate applies for a position
- Our infrastructure is designed to ensure that we minimise the risk of external cyber-attacks and system hacks
- Personally identifiable data is encrypted at rest so that should a hack happen and the candidate data accessed in some way, data is unreadable
- Any cookies that are used to monitor the user session connection with one of our servers does not contain personally identifiable data
- We regularly use an external penetration testing provider to verify our systems are secure
- We have coding and separate security coding standards so that each developer working on our systems is compliant and ensures that no security vulnerabilities are created when software is created or amended
- We use have a process of "peer review" of new software developed as well as a testing/quality department to check that our standards are adhered to
- We have a formal software Release Management and Change Control processes in place before we make any new software live
- We have rollback and backup processes in place to ensure further resilience

- We have an established and appropriate data protection policy
- We have a nominated individual as a data protection lead
- We provide data protection awareness training for all staff
- We carry our identity checking, right to work, referencing and criminal record checking for all new staff
- Our existing employees have undertaken basic criminal record checks (Disclosure Scotland)
- We are registered with the Information Commissioner's Office
- We have made privacy notices readily available to customers and candidates
- We have an established process to recognise and respond to individuals' requests to access their personal data
- We work with our customers to ensure that their established processes are sufficient to ensure personal data is of sufficient quality to make decisions about individuals
- We have an established process to routinely dispose of personal data that is no longer required in line with agreed timescales. Unless otherwise required by the Customer's data retention policy, Vacancy Filler will retain candidate data including video interviews for no more than 12 months from the recruitment campaign go-live date
- We have an information security policy supported by appropriate security measures
- We have an established process to ensure new projects or initiatives are privacy-proofed at the planning stage

## GDPR and Amazon Web Services

In February 2017 AWS announced CISPE ([Cloud Infrastructure Services Providers in Europe](#)) membership and compliance with First-Ever Code of Conduct for Data Protection in the Cloud. ISPE is a coalition of about twenty cloud infrastructure (also known as Infrastructure as a Service) providers who offer cloud services to customers in Europe. CISPE was created to promote data security and compliance within the context of cloud infrastructure services.

More details can be found here...

<https://aws.amazon.com/blogs/security/aws-announces-cispe-membership-and-compliance-with-first-ever-code-of-conduct-for-data-protection-in-the-cloud/>

Further information in general about EU GDPR can be found here [EU GDPR](#).