General Data Protection Regulation (GDPR) FAQs

1. When does the GDPR come into force?

25th May 2018

2. What is the GDPR?

The General Data Protection Regulation is a new, European-wide law that replaces the Data Protection Act 1998 in the UK. It places greater obligations on how organisations handle personal data.

3. What does the GDPR apply to?

The GDPR applies to 'personal data', which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

4. Does the GDPR only apply to European organisations?

The GDPR applies to processing carried out by organisations operating within the EU. However, it also applies to organisations outside the EU that offer goods or services to individuals in the EU OR where the behaviour of individuals who are in the EU is monitored.

5. If my organisation appoints HireRight as a third party screening provider, what is the relationship between the parties?

The relationship remains as it is currently where our customers are classified as "data controllers" and HireRight, the "data processor".

6. What is the difference between a data controller and data processor?

A data controller is the entity (or person) that determines the purposes for which personal data is processed and the nature of data processed. By contrast the data processor simply processes that data on behalf of the data controller.

All HireRight customers are employers or prospective employers of individuals and as such determine the reasons for processing data and the scope of the data processed. HireRight only processes data in accordance with instructions it receives from its customer.

7. Does that mean that my organisation is solely responsible for compliance under the GDPR?

No. Unlike the current legislation, the GDPR imposes obligations on the data processor as well as the data controller. HireRight views its relationship with customers as a partnership and has built a GDPR compliance programme that is designed to support not only HireRight's efforts but those of its customers.

8. What is HireRight doing to prepare for the GDPR?

HireRight has been working on its GDPR compliance programme for the last 18 months and all aspects of the services, systems, processes, products and contracts, have been reviewed in anticipation of the "go live" date of 25th May 2018. Some key areas that

HireRight has on focused are:

a. ISO 27001 certification obtained

b. Extensive data mapping both within the organisation and outside in respect to the use of sources to assess what personal data is held, where it came from and who it is shared with

c. Updated policies including, but not limited to:
   i. Data breach;

   ii. Candidate rights;

   iii. Impact assessments;

   iv. Vendor management

d. Updated Information Notices and Consent Forms to support lawful processing and transparency principles

e. Updated contracts with all vendors and subcontractors

f. Data processing agreement to set out relevant rights and obligations under GDPR to govern client/HireRight relationship

g. Review of all products to ensure GDPR compliance with data minimisation and accuracy principles

h. Formal GDPR training for all staff – key decision makers are playing an important role in ensuring that all staff are aware of the GDPR's likely impact embedding privacy principles into the employee culture

9. Can consent still be relied upon in the screening process?

Yes, consent remains a lawful basis for processing personal data and the HireRight systems will continue to capture this.

As you may know, under the GDPR, EU Member States are able to set some of their own rules in respect to some categories of processing and employment data is one of these. EU Member States may therefore take this opportunity to clarify the status of consent in an employment context. Germany has already issued its guidance and consent is ratified.

10. Candidates have more rights under the GDPR. How is HireRight planning to address this?

Whilst candidate rights have been extended and strengthened they should still be exercised against the data controller. With this in mind, HireRight is preparing a series of policies that will support customers in addressing such rights.

By way of example, should a candidate request a copy of their report, HireRight will direct the candidate to the relevant HireRight customer whilst concurrently letting the customer know that it has received a request for information. HireRight will then act upon the instructions of the customer in respect to the release of any information.

The nature of such rights will be outlined in the Information Notice that all candidates will see at the start of the screening process and relevant contact will be made available.

11. Do the provisions of Article 10 impact my screening programme?

Article 10 removes the ability to rely on consent if processing criminal checks for employment purposes. Instead, either the information must be gathered from a government source or there must be a law in the relevant EU Member State that allows for criminal checks to be run for employment purposes.

This may have an impact on the criminal records checks that are available from 25th May 2018.

HireRight has reviewed:

a. its product suite to establish where government source information is used; and

b. EU Member State laws that permit criminal checks for employment purposes

The majority of criminal checks offered by HireRight are government sourced and as such, provided that the check is relevant and proportionate to the role to which the candidate is applying.

We will be putting together an information sheet outlining (i) any changes to products prior to May 25th and (ii) helping guide you through what to consider if running a criminal check. Your HireRight contact will also be able to work with you to review your screening programme and to assist in facilitating any changes you may require.

12. Many of the candidates screened have global footprints. Does the GDPR still allow for data transfers?

Data transfers remain largely unaffected by the GDPR and provided that appropriate measures are taken are still permissible. Data transfers are of course necessary when screening candidates as many have lived and/or worked outside of the EU or EEA.

The methods of transfer relied upon are:

a. Consent of candidates

b. Standard contractual clauses

c. Transfers to a country with an adequacy ruling

Our US parent company is also in the process of obtaining its Privacy Shield certification, though it should be noted that candidate data processed on HireRight's UK servers would not be transferred to the US *unless* that candidate has lived and/or worked in the US.

13. How does HireRight protect the data provided to it by its candidates?

HireRight has in place state-of-the-art technology designed to protect data and has recently obtained the ISO 27001 certification. This certification evidences compliance with the GDPR requirement to have in place adequate security and technical measures.

14. Will HireRight put in place a data processing agreement?

Yes. Our contracts track current laws but all will be updated prior to 25th May 2018. We appreciate that many clients may want to use their own data processing agreements (DPA) but HireRight believes that supervisory authorities will consider one consistent programme to be best practice from a compliance perspective. We have used the Article 28 Working Party draft as the basis for our DPA and this will be circulated very soon.

15. What does the future hold?

HireRight is building a "Single Global Platform". The GDPR has given HireRight a fantastic opportunity to adopt the principle of "privacy by design": privacy is a fundamental component in the design and maintenance of information systems and the mode of operation for HireRight. The key features of Single Global Platform are:

a. Consistent background checking programmes and reporting

b. Local experience for candidates

c. Local legal and compliance requirements addressed

d. Underpinned by security and technical measures

    i. Data location

    ii. Products and processes

e. Ring-fence data residency, customer support, operations

We believe that with this design we are at the forefront of GDPR compliance.

16. Where can I read more about HireRight's efforts in respect to GDPR compliance?

Please do follow our series of blog posts "12 steps to GDPR compliance" over on https://www.hireright.com/emea/blog/category/gdpr/

HireRight Limited is a limited liability company incorporated in England (registered number 4036193) whose registered office is at Gun Court, 70 Wapping Lane, London, E1W 2RD.

Contact HireRight:
Customer Service: 0800 640 6400
https://www.hireright.com/emea/contact-us