



# The Global GDPR Countdown

How to Set up Your International  
Screening for Success

## Contents

|  |    |
|--|----|
| Foreword from Steve Girdler, Managing Director, EMEA and APAC          | 3  |
| Foreword from Caroline Smith, Associate General Counsel, EMEA and APAC | 5  |
| A Brief Introduction to the GDPR and Screening                         | 6  |
| Issues and Recommendations   | 8  |
| Case Study: How HireRight Has Created Secure Foundations               | 13 |
| 5-Step To Do List  | 19 |
| HireRight's Candidate Commitment                                       | 21 |
| Get in Touch   | 24 |

# Foreword

The amount of hugely personal data involved in the background screening process means this is one area of business greatly affected by the implementation of the GDPR. Regardless of where a candidate may be applying for work, if that candidate resides in the EU then the GDPR will apply - meaning that nearly every business will have to consider it at some point.

It may sound vexing and perplexing, but the GDPR, in essence, is about giving individuals the power to control their own data. Fairly, transparently and proportionately - which is exactly the spirit of the GDPR.

Because the candidate is central to everything we do at HireRight, we treat this regulation not as an inconvenience but as an opportunity. We are using the time until its enforcement to work with clients to put in place new procedures, ensuring candidates are comfortable and confident in the screening process. We want them to understand how their data is being used, why, who by and how it is being transferred, processed, stored and deleted.

---

“ We are all so used to talking about data from the corporate perspective, but the way I now look at it is: how would I want my own data to be handled? ”

---

That’s all very good in principle but as with any legislation, implementing the GDPR is not a simple task. It is wide-ranging and most significantly affects multinational businesses with complex operations. Any change on this level is bound to cause disruption, requiring cross border cooperation and alignment.

To help during this time, as a case study for data processors and controllers to learn from, this report outlines how we, as a data-reliant multinational business, have addressed the GDPR. I hope you find our openness and the guidance throughout the report useful.

I would like to take this opportunity to wish you the best of luck as you become GDPR-compliant. Do get in touch if you have any further questions at all.



**Steve Girdler**  
HireRight Managing Director  
EMEA and APAC

Being ready for the GDPR to come into play is a challenge for any international company, requiring an entire review of how data is processed during a recruitment process that spans the whole world. It is complicated further by the fact that there are no hard and fast rules. For one thing, the regulations are principles based rather than being a list of actions. Consent, data mapping, subject access rights, privacy impact assessments: these are all weighty legal issues, and without any black and white answers on the right thing to do, the GDPR minefield can seem overwhelming.

In addition to this legal complexity, most EU countries are yet to outline any local differences (known as derogations), making it difficult to make concrete long-term plans.

The regulator will not allow derogations that diverge significantly from the overall rules. So, my recommendation? Take affirmative action now and document your reasons for taking such actions. Wait until everything is absolutely clear and you will be too late to adopt changes.

---

“ The more you know about the GDPR, the more you know it leaves many questions unanswered. But the idea of the GDPR is that it provides a level playing field.

---

With the countdown on, what do businesses need to do to ensure their international screening is GDPR-ready? To help those grappling with this question, we organised a roundtable discussion with risk and HR leaders to find out their key concerns as we approach the implementation date. This paper

summarises the key questions that were raised about the GDPR during screening and reveals our recommendations on how to address each.

I hope you find it useful over the coming months and beyond, as new derogations and developments are revealed.



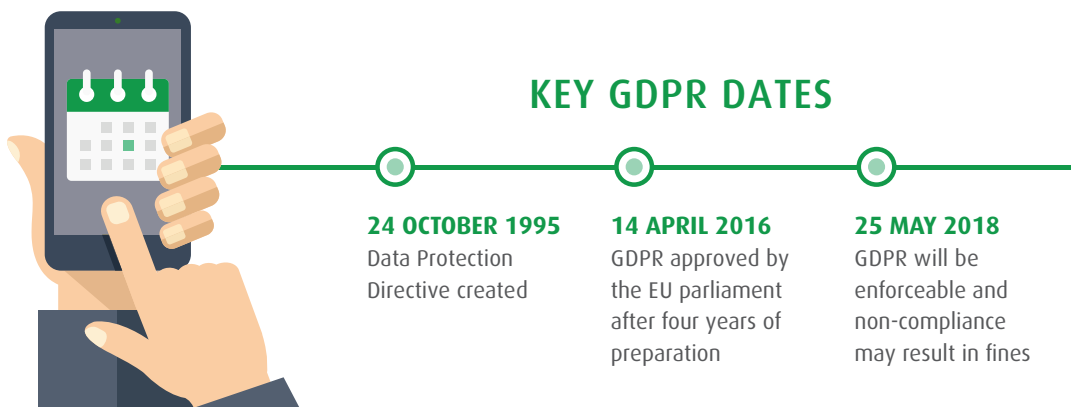
**Caroline Smith**  
Associate General Counsel  
EMEA and APAC

# A Brief Introduction to the GDPR and Screening

The EU's General Data Protection Act, more commonly referred to as the GDPR, is designed to:

- **Protect people's data and give them the power to control it**
- **Ensure businesses take data protection seriously and embed privacy within the fabric of those businesses**
- **Create alignment across the EU**

It affects any company that deals with the personal data of EU residents, whether they are citizens or otherwise – in other words, most businesses today.



Failure to comply could result not just in negative publicity but also business-altering fines of either €10 million or 2% of annual global turnover or €20million or 4% of annual global turnover (in each case whichever is greatest) depending on the type of breach.

With less than a month until its final implementation, businesses, not just in Europe but across the world, are putting in place the processes and procedures that will ensure compliance.

It's been on the horizon for years, but are businesses ready?

- **In the US, 92% of businesses list GDPR as a top data protection priority (PwC)<sup>1</sup>**
- **69% of EMEA HR professionals believe their organisation is fully prepared and knows exactly how to comply (HireRight)<sup>2</sup>**

But this confidence may well be misplaced.

- **Only just over a quarter of businesses have made changes to their operations in response to the GDPR (UK government)<sup>3</sup>**

This an incredibly low figure considering the regulation's scope. So, what are the issues businesses should be considering? And how should they go about addressing them?

# Issues and Recommendations



At our roundtable event in January 2018, these twelve key questions were raised by HR and risk professionals from multinational organisations. The answers were debated, and the following recommendations made:

### **1. Are there differences across geographies?**

There are limited places where local regulators can make changes to the GDPR. In particular, they can't alter how data processing agreements (DPAs) are understood as the agreements are required to contain all the principles under Article 28 of the GDPR: this is the key part of the regulation for screening as the DPA governs the relationship between the data controller and the data processor. While there may be minor differences between how different member states implement the rules, these derogations should not prevent action.

### **2. Will we know by May which countries will derogate?**

We are monitoring all the EU member states to see what they're going to come out with, particularly around criminal checks which is where there is the biggest discrepancy between country's legislation at the moment.

### **3. Will Brexit impact the GDPR?**


The UK will have to comply to the regulation until it leaves the EU. The UK government has gone on record to state that post-Brexit, any new law adopted will be the same as or closely mirroring the GDPR and that a ruling of adequacy will be sought to allow "safe" transfers of personal data. To this end, the UK Government has already issued the UK Privacy Bill. You should treat the UK as you would the rest of Europe, though you may want to include reference to it in consent forms to make it clear that the same standards will be adhered to.

### **4. How should consent be obtained?**

Ensuring candidates genuinely consent to screening is about holding the hand of the candidate all the way through the screening process. They must be asked if they consent, of course, but that is not enough. You should take every opportunity to make sure candidates understand the process and that they can back out of it. We also recommend that if you have Work Councils, you should discuss screening with them to ensure that they are on board with what you are doing, as this will reassure candidates.

## 5. Is consent needed for rescreening?

Consent must be for a specific purpose and you should not re-use consents to process old data for a different purpose. Arguably any rescreen would fall outside the original consent given and as such you will need to ask for consent again. However, given that many rescreening programs are dictated by regulation, such as the Financial Conduct Authority rules, it may be possible to rely on other forms of lawful processing such as “legitimate interest” or where a rescreen arises purely from an internal Human Resources policy, “fulfilment of a contract in favour of the data subject”. HireRight is looking into both options for any rescreening solutions.

 [Read more on the best steps to gaining candidate consent](#)

## 6. How long should data be retained for?

It should only be held for as long as necessary. Businesses usually want to hold onto data for as long as possible, but if you currently have long retention periods (anything over 6-12 months) you should consider reducing these. This will reduce the risk of candidate claims and fines: if you don't hold data then there is nothing to disclose, remediate or expunge should a candidate exercise any rights. If a candidate wants their data to be deleted immediately, that should also be allowed.

## 7. Do companies need to share screening data with candidates if they ask to see it?

Yes, it's unlikely businesses will be able to provide a defence not to. That's why you should ensure that data is accurate and contains no opinion - even from references.

## 8. What information should be shared with candidates?

We recommend mapping out the candidate journey to work out when, where and what to communicate.

Consider...

### **An initial communication outlining:**

- The overall process and timings
- What data is usually sourced at this level of responsibility and how
- How data is stored and moved
- Relevant rights

- How to opt-out
- Who to ask for more information

**A follow up communication outlining:**

- More specifically the process for the role in question

**A final communication outlining:**

- The outcome of the screening and next steps


It is also wise to ensure more detailed information is available at each stage, for instance, some people may want to know who you will ask for information. When a candidate comes in, you won't know where they've lived so you can't say immediately where you will source their screening information from. Consider how you would develop a visual infographic including sources of data (if that's not confidential) and the type of data that will be sent to that source to perform the check. This will be too much information for most people, but you should know how to do this for those that do make a request.

**9. Can people withdraw from the process at any point?**

Yes, and all relevant rights - including the Right to Withdraw Consent and the Right to be Forgotten - should be outlined in the consent forms. There could be various reasons why they want to withdraw consent. It could be that they've decided to withdraw from the whole process generally. It could be that they've got cold feet. Or they might have something they're worried about and that they want to talk to you about before you find it out. If you put a pause on screening and allow a dialogue to happen, most of the time the screening will continue afterwards.


**10. How can businesses address the Right to be Forgotten?**

The information that a candidate might want to be forgotten is unlikely to be held solely by you. Making data sources available to candidates means they can go directly to where the information is being held in order to address it.

 **Read more on how to deal with the Right to be Forgotten**

## 11. How relevant is data residency to the GDPR?

The GDPR does allow you to transfer data but conversely the GDPR gives candidates more rights and freedom to exercise their voice in respect of the choices they want to make as to where data is processed. Therefore, if a candidate is uncomfortable with a process, they are more likely to drop out, so it's important to think about where data is going and why. When a candidate is being screened ahead of their employment, if they have always lived and worked in the UK, they would not expect their data to go to the US just because that's how a potential employer has set up their screening processes.

 [Read more on how to carry out data transfers under the GDPR](#)

## 12. How can companies help candidates feel more comfortable about screening? Will all this information make them more nervous?

Communicating the right information at the right time and in appropriate depth will help candidates to have a better understanding of how the process works and allay fears. It should be clear that even if a discrepancy is found, you will discuss it with them before making a decision.

---

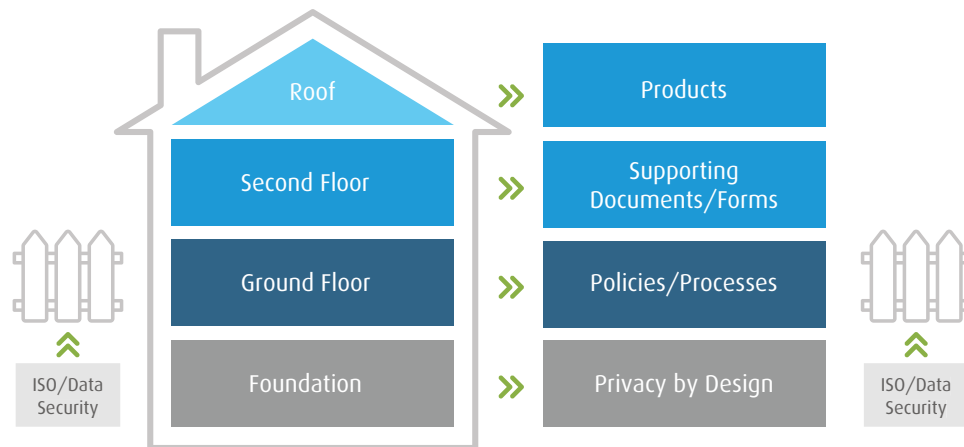
“ At the very beginning of the recruitment process, it's important to explain why you carry out background screening. It can be done very positively because it's not just about determining whether someone is a risk but also safeguarding people - it needs to be demystified. Having this visibility around regulation could actually make the whole process of screening less scary and unknown - putting the power back into the hands of individuals.”

- Steve Girdler, HireRight Managing Director EMEA and APAC

# Case Study

## HireRight: How We Have Created Secure Foundations

**Whether you are a data processor or controller, you need first-rate security intent measures. Here's how we approached the challenge:**



### Mapped Data Flows

Our first step was to create an official map of where data comes from and moves to during the screening process - how does candidate information get into our system and, once it's in there, where does it go? This isn't as simple as it might sound, having to take into account clients, vendors, sources, candidates and laws from across the world.

[Read more on how to data map your background screening process](#)

Once we had it mapped, we could work out how we could improve how we move all that data. We also used it to categorise our vendors in terms of the sensitivity of the data that they handle, to ensure they all adhere to the same high encryption standards.

[Read more on vendor management best practice ahead of the GDPR](#)

### Achieved ISO Certification

To make it clear how seriously we take data security, we applied for and gained the respected ISO/IEC 27001:2013 certification. Any size or type of business can apply for this accreditation, which according to the independent standard setting-body, ISO, proves that an organisation is "establishing, implementing, maintaining and continually improving an Information Security Management System".

Becoming certified to ISO 27001 provides independent assurance that our Information Security Management System has been tested and audited in line with internationally-accepted standards. It provides guidance for implementing appropriate measures to mitigate risks, with recommended technical measures in line with the requirements of the GDPR. It also promotes a culture and awareness of information security that makes sure data security is entrenched across the business.

HireRight's Information Security Manager for EMEA and APAC believes the accreditation is a valuable step as firm evidence of the real quality of your data operations: "The ISO certification is wide-ranging, covering everything from password management and access control to network security. It's not easy to achieve, requiring a number of stages of information collection and audits which ensure your processes are robust, controlled and clearly managed.

"What's really important about this certification is that it's about the ongoing management of systems. It's not a one-off, 'let's tick that off the list' award, but a standard to be upheld as the security landscape continues to change at a pace. We used it as a template so that we knew we were delivering exactly what was required and now we are building on that even further to ensure that our information security management is second to none."

### **Carried out Data Privacy Impact Assessments (DPIAs)**

Data controllers are required to carry out DPIAs. A vital part of the idea of 'Privacy by Design', they are a tool to make sure that privacy and data protection is a key consideration when sharing data - and that risks to EU citizens data are highlighted and addressed.

Because data is so integral to everything we do, we have decided to carry out DPIAs across almost the whole business and will continue to do so as the GDPR and our understanding of the regulation develops.

 [For more on DPIAs please read our blog on when and how to carry them out](#)

### **Improved Our Policies and Procedures**

Our services are quite esoteric; our clients are not simply outsourcing payroll. We've been looking at how we carry out criminal checks, media checks and references to

make sure we are focusing only on information that potential employers need to know about.

We reviewed the full candidate journey and asked ourselves, “What can we do better? How can we make sure everything that we do is clear, transparent, open and fair?”



The International Organisation for Standardisation (ISO) is an international standard-setting body composed of representatives from various national standards organisations. Founded in 1947, the organisation promotes worldwide proprietary, industrial and commercial standards. ISO 27001 is the international standard which is recognised globally for managing risks to the security of information you hold. ISO 27001:2013 (the current version of ISO 27001) provides a set of standardised requirements for an Information Security Management System (ISMS).

### Ring-Fencing EU Data

At the heart of the GDPR is putting control of personal data back into the hands of the individual. Everyone, under the regulations, has the right to determine what personal data is used and how and where it is processed and transferred. In practical terms, if a background screening company is processing the data of an individual for the purposes of employment on behalf of a third party – the employer – the individual has the right to refuse his or her data being transferred or processed outside of the EU.

This means that data processors, such as background screening companies, need to be able to demonstrate systems, processes and IT design that ensure that no personal data, other than that which is pertinent to a particular check, is transferred outside the EU. This includes customer service representatives viewing files with personal data. With greater controls and rights for data subjects and their personally identifiable information, HireRight has integrated the ability to ring-fence the



storage of EU nationals' data to within our EU data centres. This ensures it meets the conditions laid out in the GDPR for the protection of their information.

### Created Supporting Documents

Until now, people were given the option to opt-out of screening at the very start and were made aware that their data wouldn't be sent beyond the EU. That just doesn't go far enough anymore.

To meet the principles of the GDPR and our own commitment to be as clear and transparent as possible, in our supporting documents, we now invite candidates to read much more information and to get in touch if they've got any questions. We tell them who's screening them and why they're being screened. We let them know where their data might go, when and the sources of information. This helps candidates to feel safer and more secure about the process.

We have adopted a layered approach to information to strike the balance between providing full, clear and transparent information vs. overloading a candidate with information: this means that a candidate can explore the various levels of information as they wish, with the aim of providing the right level of information at both ends of that spectrum, readily and easily available.

### Updated Consent Forms and Privacy Policies

To help our clients with their obligations as data controllers, we're preparing for candidate queries about the rights to be forgotten, for access and to erasure.

We've also agreed our breach notification policies. There are narrow time frames imposed by GDPR and we want to know the exact process to correct issues and communicate with clients and candidates.

We're making sure that we have strong data processor agreements in place with all our clients so that the regulators know how we are working together.

 [Read more on how to prepare for data breaches](#)

### **Offered Aligned Products and Services**

We've got an increasingly global workforce with increasingly complex legislation, so we are creating a single global platform that delivers consistent results and ensures clients have an entirely level playing field in how they are assessing candidates.

### **Next Steps**

We're rolling out internal training to all our staff on the GDPR - whether they are directly affected or not. We'll be keeping that going over the coming years as the regulation and our approach to it develops.

# 5-Step To Do List

## 5-Step To Do List

- 1** Map out where data flows in your organisation and between your vendors and partners. Address any and all issues this highlights.
- 2** Carry out DPIAs wherever appropriate across your organisation and at the start of every data-related project.
- 3** Put in place thorough communications covering the entire candidate journey.
- 4** Make sure your vendors know what is expected of them - and that you as a vendor know what your clients and customers expect of you.
- 5** Have in place a thorough and easy-to-find policy for all eventualities.

# HireRight's Candidate Commitment

We make these eight commitments to every candidate that we screen.

**1. We will protect your data to the highest standards.**

We know you care about your personal data being safe because we each feel the same way. Our information security management is ISO/IEC 27001:2013 certified and we use the industry's most compliant and up-to-date software and hardware.

**2. We will be clear and transparent about how we process your data.**

We will communicate what data we will process, who will see it, how we will transfer, process and store it and when it will be deleted. Once you have told us where you have lived and worked, we can also tell you exactly who we will contact to confirm your details.

**3. We will take into account local laws and customs when performing checks.**

The checks that are offered to employers have been vetted to ensure that they are lawful in the country they are offered. The HireRight teams will also work with its employers to guide them through choosing checks that are appropriate to the role you are applying for.

**4. We will make sure you know your choices and status at every stage.**

We want you to be able to make an informed decision about whether you are comfortable with the process. We will give you the opportunity to opt-out of screening - and then you can opt-out at any stages later on too.

**5. We will not share your data more widely than necessary.**

We'll ensure your data is only sent to a jurisdiction in which we are performing a check, otherwise your data remains in your region - whether that is EMEA or the Americas, unless you are being screened for a role in another region.

**6. We will be impartial.**

We do not decide whether you are hired nor do we make any recommendations to hire to your potential employers: this is the choice of the company who you have applied to work for. To help them make a fair and accurate decision, we ensure that the reports we produce are based on facts and never opinion.

### **7. We will be open.**

If you wish to see your full screening report, you can request it from your prospective employer. HireRight will work with them to ensure that this process is swift and transparent.

### **8. We will make it as easy as possible to use our service.**

Your time is valuable to us and we know your prospective employer may be asking for a great deal of information. Our goal is to make the process as user friendly, straightforward and as fast as possible. We will answer your questions quickly and provide innovative tools to complete the process without delay.

# Get in Touch



**If you need any more information on how to guarantee your global screening program is GDPR-ready, get in touch.**

### Steve Girdler

Managing Director, EMEA and APAC

@ Steve.Girdler@hireright.com

+44 207 264 6265

+44 7780 606006

@SteveGirdler

uk.linkedin.com/company/hireright

@HireRight

emeasales@hireright.com

<sup>1</sup><https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html>

<sup>2</sup>HireRight EMEA 2018 Employment Background Screening Benchmark Report

<sup>3</sup><https://www.gov.uk/government/news/digital-and-culture-secretary-urges-businesses-and-charities-to-prepare-for-stronger-data-protection-laws>

## About the Report

The Global GDPR countdown: How to Set up Your International Screening for Success is based on insights from a roundtable held by HireRight in January 2018, featuring senior representatives from a selection of multinational organisations.

## About HireRight

HireRight is a leading global provider of candidate due diligence services - background screening employees and job applicants to help organisations mitigate employee risk, make informed hiring decisions and meet compliance obligations.

HireRight works in more than 200 countries and territories, and has offices across the globe, including the UK, USA, and Hong Kong. Almost half of the Fortune 100 and over a quarter of the FTSE 100 use HireRight's services.

Find out more at [www.HireRight.com/emea](http://www.HireRight.com/emea)

This report and its contents are the property of HireRight Ltd. HireRight Ltd is registered in England under company number 4036193 and whose registered office is at Gun Court, 70 Wapping Lane, London, E1W 2RD.

This HireRight report is provided for informational purposes only and should not be construed as legal advice. Any statutes or laws cited in this article should be read in their entirety. If you or your customers have questions concerning compliance and obligations under United States or International laws or regulations, we suggest that you address these directly with your legal department or outside counsel.