# The impact of GDPR on background checks

Zinc

# The impact of GDPR on background checks

**by Hamraj Gulamali**

FEBRUARY 2023

# Introduction

This white paper is complementary to the webinar delivered on the same topic on Wednesday 1st February, the recording of the webinar can be found here. In combination, the white paper and webinar are intended to act as an aide for HR professionals trying to navigate the complexities of the General Data Protection Regulations (GDPR) and the United Kingdom General Data Protection Regulations (UK GDPR) in a post-brexit and post-pandemic world.

This white paper is split into five sections, firstly the practical impact of having two regulatory regimes following the United Kingdom's (UK) exit from the European Union (EU) shall be discussed. Secondly this paper shall consider the impact of GDPR on right to work checks before moving on to the third section where the importance of candidate specific privacy policies shall be discussed. The fourth section shall consider criminal background checks in the UK and EU before finally, this paper shall offer some brief concluding remarks.

SECTION 1

# A duality of regimes

GDPR was adopted in the EU on 16th April 2016 and became enforceable on 25th May 2018. Concurrently the UK voted to leave the EU on 23rd June 2016. The decision to leave the EU was followed by a protracted negotiation period between the EU and UK and the withdrawal was not completed until 31st January 2020. The formal withdrawal was followed by a transition period and UK GDPR did not come into effect until January 1st 2021. On the day UK GDPR was adopted it was almost a verbatim copy of GDPR but it has subsequently developed and the two regulatory regimes now differ in places.

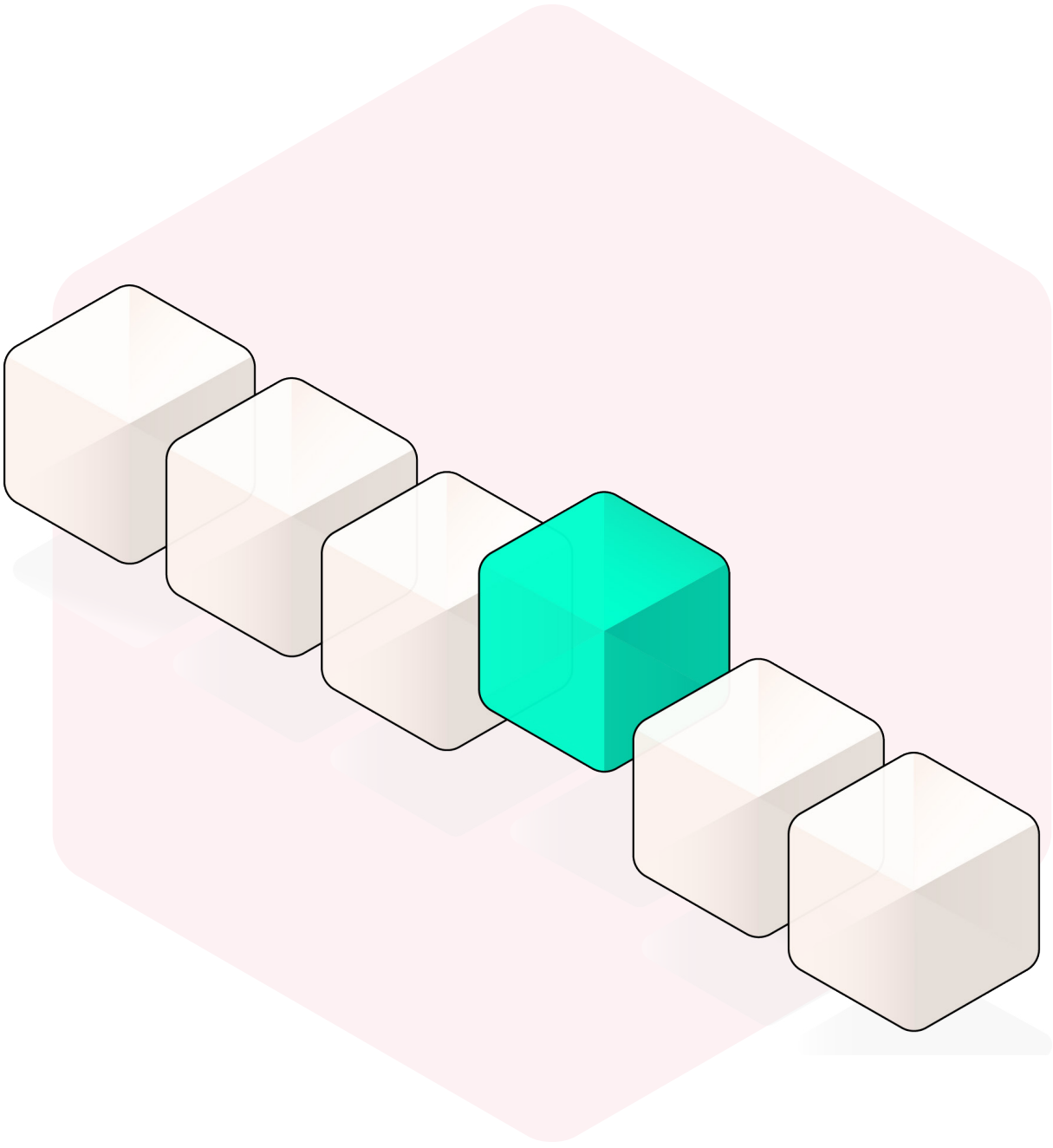
To add to this convoluted timeline is the nature of enforcing GDPR across the EU. The EU comprises twenty seven member states and importantly, each member state has its own data protection authority. These authorities are responsible for, amongst other things, enforcing compliance with GDPR and punishing non-compliance. Each authority is therefore tasked with interpreting GDPR, responding to breaches and doling out punishments. There is some uniformity across the Union but regional variations persist in many areas.

Further, the law typically requires time and stability before certainty can develop. GDPR is just under seven years old and has only been enforceable for a little under five years. It has been tested in certain places and as will be explained below, there are some areas of clarity, however, our understanding of the practical impact of GDPR is still developing. It is not always easy to say with certainty how a specific data protection authority will react to a given non-compliance.

This must be coupled with the UK's decision to leave the EU which in real terms means that UK GDPR has had little over two years during which it has been tested. The UK's data protection authority is the Information Commissioner's Office (ICO) and given the aforementioned complexities, it is not always clear how the ICO will treat incidents of non-compliance.

These complexities are all the more important for employers given the de facto position that they assume under GDPR. Employers will always be considered Controllers in relation to their employees, this is unsurprising. More interestingly, there is a de facto presumption that any third party provider will be deemed a Processor under GDPR. For employers using a third party background checking service such as Zinc, the de facto presumption comes into operation. Employers will be considered the Controller and companies such as Zinc deemed as Processors. This situation puts the onus on employers to ensure compliance with GDPR. Naturally where a Controller can point to a contractual obligation on the part of their Processors to comply with GDPR and where factual evidence can be adduced of a Processors failure to do so, the Controller will have the basis of a claim against their Processor. However, as with any litigation, the outcome of that claim would be far from straightforward.

All of the factors discussed in this section demonstrate the importance for employers to ensure that their background checking process is compliant with GDPR. With that established this paper shall move on to discuss three aspects of the background checking process and consider the privacy related implications.



SECTION 2

# The pursuit of privacy

**Privacy and immigration laws**

Right to work checks are the bread and butter of the background checking process. Zinc for example runs background checks for nearly three hundred clients. Between them they conduct a variety of checks but every one of them chooses to conduct right to work checks.

The reason for this is clear when the two most important interests are considered. The first interest is the employee or candidate's right to privacy. This must be measured against the employer's obligation to verify that a given candidate or employee has the legal right to work.

Article 8 of the European Convention on Human Rights (ECHR) enshrines any natural person's right to privacy and this is given effect in the UK by the Human Rights Act 2018. Importantly this is not an absolute right and the interplay between the right to privacy and a given jurisdiction's immigration laws has always been part of the equation.

In the UK, section 35 of the Immigration Act 2016 creates an offence for an employer to employ a person they know or have "reasonable cause to believe" has

no right to work. Similar provisions exist across the EU. Currently there are no known cases of a claimant successfully invoking their Article 8 right to privacy to prevent them undergoing a right to work check in line with local immigration laws. It is opined here with some confidence that such a claim is unlikely to ever be successful in England.

**Storage of RTW data**

With regards to Right to Work checks and GDPR, the biggest issues arise after the check has been completed. Again, the reason for this is understandable when the competing interests are considered. In this case the interests are the GDPR recommendations which must be measured against an employer's practical obligations to its employees and the wider company.

Article 5(1)(e) of the GDPR states that data which could identify a data subject should be kept "no longer than is necessary" for the purposes the data is required. This can be contrasted to three classical use cases that employers regularly deal with.

**Recruitment processes**

During a recruitment process employers collect personal data on candidates, once the recruitment process has been completed then following GDPR guidance the data should be deleted as it is no longer "necessary". As an employer however, this may not be practical. Firstly, those working in Talent Acquisition will be well aware that recruitment processes are far from straightforward. Data might be kept for at least a few months in case a candidate drops out of an agreed role or a new role opens up within the organisation on short notice. Further, there is the outside possibility that candidates may bring a claim for discrimination during the recruitment process pursuant to the Equality Act 2010. Claimants have six months to bring such claims and so employers are advised to keep candidate data on file for at least six months despite it no longer being strictly "necessary".

**Payroll data**

Employers require financial data on their employees, for example, payroll data to ensure they are paid correctly and on time. Financial data is not considered special category data under GDPR, however, it is opined here that data breaches involving

financial data (such as credit card details) are more likely to receive higher penalties when considering the Article 83(2)(a) GDPR factors for assessing the seriousness of a breach. Given this, it would be recommended that employers delete financial data as soon as possible. Clearly in the case of payroll data, which is required monthly, this deletion is not possible. It is advised that employers consider these ramifications carefully when deciding how best to store financial data.

### Employee data

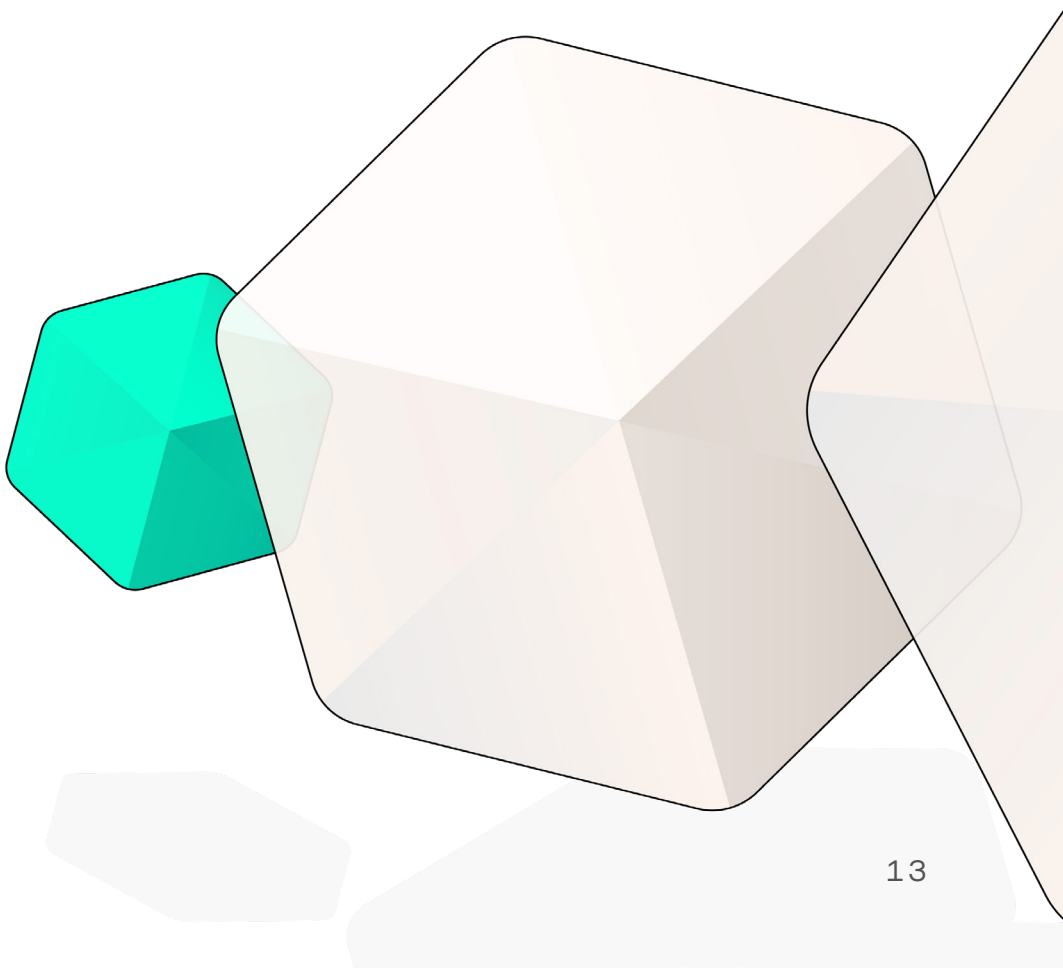
On a related point to payroll data is general employee data such as contracts or performance reviews. Following the GDPR recommendations then the most natural point to delete such data would be immediately after an employee ceases to be employed, regardless of the reason. However, employees can bring claims in the employment tribunal against their employers for up to three months after the date of termination. More interestingly, there is nothing technically stopping an employee from bringing a claim in the general civil courts in England and Wales. Such a claim would only be time barred by the statute of limitations which in this case, would run for six years.

Instinctively it may be thought that

a judge would look unfavourably on such claims brought outside of the employment tribunal system, however, the process of collecting evidence that can substantiate a claim may be onerous and time consuming. As such, employers should be alive to the possibility of defending a claim some years after the date of termination, especially in cases of acrimonious terminations.

When considering the storage of employee data, these three use cases demonstrate that each employer must carefully consider their own obligations to employees and the wider company.

Further, they must consider these obligations in light of their specific industry requirements and day to day business needs before settling on retention and deletion policies.



SECTION 3

# Moving beyond standard procedure

Candidate Privacy Policies or Recruitment Privacy Policies (CPP) are coming into vogue in addition to regular Privacy Policies. On first glance this may sound counter-intuitive when the contents of a CPP are considered. In regards to candidate data a CPP would set out what types of data is collected, how the data is collected, why the data is collected (including legal basis for doing so), who in the company has access to the data, how it is stored and what the data subject's rights are in respect to the data.

On the surface, this appears almost identical to a regular privacy policy. However, this paper advocates for the use of CPPs in addition to regular privacy policy on the basis of the extra specificity they provide.

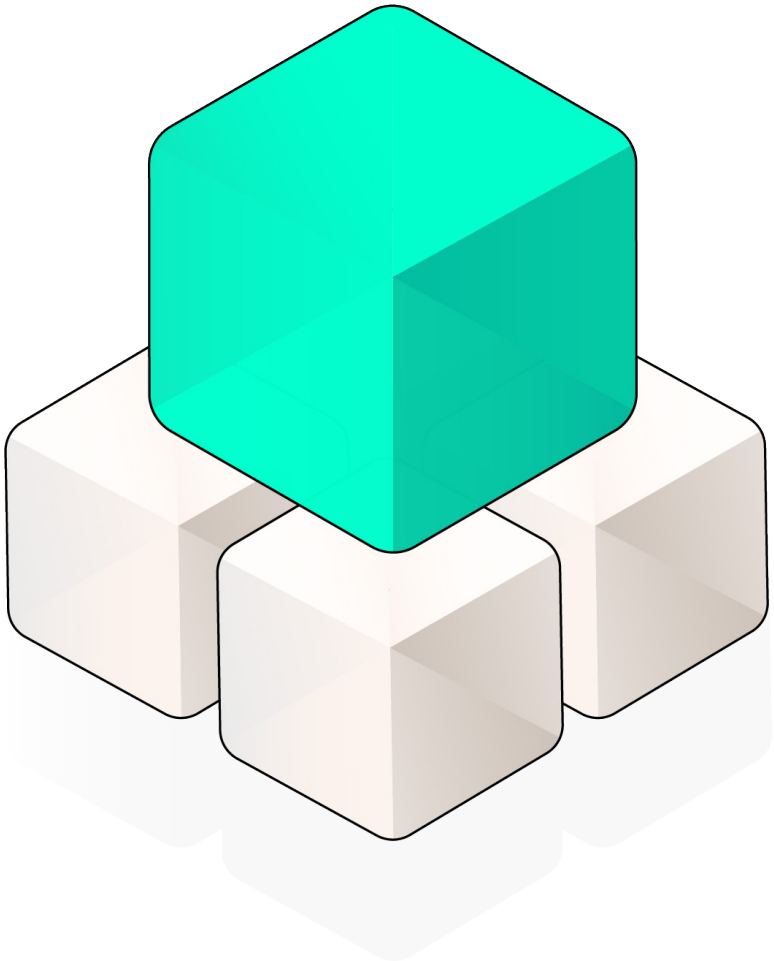
When assessing most privacy policies it becomes apparent that many companies rely on their "legitimate interest" to collect data through the general use of their services. Legitimate interest is the most flexible ground for collecting data that a company can rely on. Per the ICO it is most likely to be appropriate when using a natural person's data in ways they would reasonably expect and which would have minimal privacy impacts (i.e.

email addresses for correspondence not marketing). Whilst flexible, legitimate interest is also a weak basis to rely on because it lacks specificity without which it could be easily overridden by a data subject's privacy rights.

In the course of conducting a recruitment and background checking process employers collect significant amounts of personal data, some of which may be akin to sensitive data for the purposes of GDPR (e.g. criminal background data). Importantly, employers have full justification for collecting such data. For example, general personal data would be collected to ensure a fair and robust process for all candidates. Education verification checks and credit checks might be used to verify the integrity of their workforce. Lastly, employers might require criminal background screening to ensure the safety of their workplace. All of these would entail the collection of personal data.

More importantly, all of these are perfectly valid reasons for an employer to require data from their candidates. The advantage of using a CPP is that it allows employers to clearly spell this out. It bakes in a robust policy which can be pointed to in the case of any alleged non-compliance on the part of a data subject or a data protection authority.

In sum, given the types of data collected by employers and the valid justifications for doing so, the use of a CPP is highly recommended. The ease of using a catch all privacy policy is not disputed. However, it is opined that the use of standard privacy policies to cover wide reaching data collection and processing activities is in the long term likely to be seen as unsound. Companies should begin the process of decoupling their reliance on them as quickly as possible.



# Convictions across the Union

Criminal background checks are easily the most contentious area of law and this is apparent from the regulatory framework. Article 10 GDPR states:

> Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

(2) Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

In essence this defers authority to Member State law given that there is no Union law which authorises the processing of criminal conviction data. The practical effect is that there are twenty seven different interpretations of what is acceptable in regards to the processing of criminal conviction data which must be considered alongside the UK's regulatory regime.

Space does not permit a full exploration of these regional variations and so this paper shall end with three practical tips that employers in the UK can take to protect themselves in such a complex landscape.

Firstly, it is highly recommended that employers conduct a Data Protection Impact Assessment (DPIA) if they choose to conduct criminal background checks as part of their recruitment process. The ICO requires DPIAs to be conducted when collecting criminal conviction data on a "large scale", unhelpfully guidance is not provided as to what a "large scale" is. As such it is recommended that DPIAs be conducted for the processing of any criminal conviction data.

Secondly, it is highly recommended that employers have a CPP documenting why they need to collect criminal conviction data. Thinking back to Section III of this

paper, one justification for collecting criminal data could fall under the banner ensuring the safety of the workplace. What is important is spelling this out clearly in a CPP. It would not be overkill to have a specific section within a CPP devoted to the collection of criminal background data. This would cover bases with data subjects, data protection authorities and potentially assist in any claims for discrimination brought against employers.

Lastly this paper recommends developing a strong record keeping process detailing why criminal conviction data is required, how long it will be kept for and which employees have access to it. Note this is separate to a CPP, record keeping is its own area that requires just as much attention. Lastly, ensure that employees are sticking to the policy by regularly monitoring compliance through recurring training sessions, not just during onboarding.

# Conclusion

This paper is intended to assist HR professionals seeking to navigate the complexities of GDPR and its interplay with the hiring and background checking process. To that end this paper has discussed the practical implications of having two GDPR regimes across the EU and UK and explored the importance of ensuring compliance for employers. This paper then moved on to consider the impact of GDPR on right to work checks and the tension between privacy rights and immigration laws. This was followed by an examination of CPPs before finally this paper briefly addressed criminal background checks and offered some advice for employers conducting them.

If you have any further questions please do not hesitate to reach out to the Zinc team. We are happy to help with any and all of your GDPR related queries arising out of our webinar and white paper series.

hamraj@zincwork.com