

Asking the question

Guidance for employers on the GDPR, data protection and the processing of criminal records data in recruitment

Written by Rachel Tynan and Christopher Stacey

First published: October 2018

Contents

Summary.....	3
Introduction.....	4
Section 1: Background	5
The GDPR and the Data Protection Act 2018.....	5
Data protection principles.....	5
Criminal record disclosure rules.....	7
Asking applicants to self-disclose.....	7
Carrying out official criminal record checks.....	7
Current recruitment practice.....	8
Asking individuals to self-disclose.....	8
Carrying out criminal record checks.....	8
Section 2: Ensuring compliance	9
1. Defining the purpose of collecting criminal records data.....	9
2. Identifying a lawful basis and a condition for processing.....	10
Part 1 – Identifying a lawful basis for collecting criminal records data.....	10
Part 2 – Identifying a condition for processing criminal records data.....	11
Selecting a lawful basis and meeting the condition for processing.....	11
3. Setting out your privacy policy and data subject rights.....	12
Examples of existing policies.....	13
Supermarket.....	13
DIY retailer.....	15
Section 3: If and when to ask	17
Asking about criminal records on application forms.....	17
Automated decision making.....	17
Asking at job offer stage.....	19
Carrying out official criminal record checks.....	19
Section 4: Conclusion	21
Employers should join Ban the Box.....	21
What’s wrong with the box?.....	22
Annex A - Checklist.....	23
More information and useful resources.....	24

Summary

This guidance is designed to support employers to ensure that their policy on collecting criminal records data is compliant with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18).

Too often, employers overlook skills, experience and qualifications if an applicant declares they have a criminal record. We encourage you to think about whether you need to collect criminal records data. This guidance makes it clear that collecting at application stage is unlikely to be compliant with the GDPR and the DPA18, but employers should also think about why they are asking at any stage. To ensure compliance, employers must demonstrate that processing criminal records data is **necessary** at whatever stage they decide to collect it. If processing is not necessary, it is not compliant.

Your organisation may have a policy on recruiting people with convictions – whether that be an inclusive policy or a blanket ban. Whatever your approach, if you are using criminal records as part of your recruitment practice, you should have a policy in place on collecting applicants' personal data, and this should include a specific section on the processing of criminal records data. Your policy should clearly identify the purpose of collecting criminal records data, the lawful basis for collecting it, and explain how long you will retain this data, who it will be shared with and the applicants' legal rights in relation to their information.

Unlock recommends employers follow a three stage process to setting out their approach to processing criminal records data. To ensure compliance with the GDPR and the DPA18 you should:

1. Define the purpose of collecting criminal records data
2. Identify a lawful basis and condition for processing
3. Set out your privacy policy and data subject rights

Key points in this guidance are that:

1. Collecting criminal records at application stage is unlikely to be necessary and therefore in breach of the GDPR and the DPA18
2. Collecting criminal records at *any* stage must be justified by a link between purpose and processing.
3. You must identify a lawful basis for processing AND meet a condition of processing
4. Applicants have data subject rights that must be upheld
5. Explaining how you will uphold applicants' rights is essential to GDPR compliance

We hope this guidance helps employers to review their approach towards criminal records and ensure that if information is collected, it is used fairly and only where necessary.

Introduction

This guidance is for employers and voluntary organisations in England & Wales who currently (or may in the future look to) collect criminal records data for recruitment purposes. The aim of this guidance is to ensure that employers understand the implications of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18) on the way that they collect, process and store criminal records data as part of their recruitment and HR processes. The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA18). The main provisions of this have applied like the GDPR, from 25th May 2018.

Unlock regularly engages with the Information Commissioner's Office (ICO) and they have contributed to the data protection content of this document. The document also contains hyperlinks to relevant ICO guidance.

This guidance is aimed primarily at employers but is also applicable to organisations recruiting volunteers - for the purposes of data protection, volunteers would generally be regarded the same as employees. Much of the content is also relevant to organisations collecting criminal records data from individuals for other purposes, such as education, housing or insurance.

The full implications of the GDPR are still being considered and this guidance will be updated as the change becomes embedded. A key change resulting from the GDPR and the DPA18 is the obligation of data controllers to be **accountable**. This was present in the 1998 Act but has a far stronger emphasis now. This means employers must **demonstrate** compliance with the data protection principles, including transparency about how and why information is processed, and an individual's rights to access, amend or erase their personal data. This is covered by the accountability principle.

Throughout this guidance, we refer to:

1. Employers – this is used to cover organisations that recruit staff directly, act as intermediaries, recruit volunteers, provide professional status, or some form of regulation to workers.
2. Criminal records – the GDPR and DPA18 use the term 'criminal offence' data. This guidance refers to 'criminal records data', which is used to cover criminal convictions, other court disposals, and police cautions.

Section 1: Background

The GDPR and the Data Protection Act 2018

The [General Data Protection Regulation](#) (GDPR) came into force on 25th May 2018 and changes the way personal data is protected in the UK and across Europe. The [Data Protection Act 2018](#) (DPA18) has replaced the Data Protection Act 1998 and contains provisions specific to the UK and also exemptions from the GDPR.

The GDPR applies to '[controllers](#)' and '[processors](#)'. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you; for example, to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. If you are a controller, the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR. It is up to each party to understand where their responsibilities are. For employers, this means ensuring recruitment agencies or online application portals are compliant with the law. Employers who manage recruitment in-house are controllers.

The GDPR and the DPA18 applies to the processing of all personal data. Criminal records data (including convictions, cautions and allegations) are a separate category of data – "[criminal offence data](#)" – and there are particular safeguards to be aware of if you collect this information as part of recruitment.¹

Data protection principles

Article 5 of the GDPR sets out [seven key principles](#) for the processing of personal data. These are listed below, with key elements that help to explain what they mean.

- a. [Lawfulness, fairness and transparency](#)
 - a. Identify a 'lawful basis' (under Article 6) and a 'condition for processing' (under Article 10)
 - b. Ensure you do not do anything with the data in breach of any other laws
 - c. Use the data fairly, and in a way that is not unduly detrimental, unexpected or misleading
 - d. Be clear, open and honest with people from the start about how you will use their data
- b. [Purpose limitation](#)
 - a. Be clear about the purpose of processing from the start
 - b. Record the purpose/s of processing and specify in your privacy information
 - c. Only use data for a different purpose if compatible with the original purpose, with explicit consent, or with a clear basis in law
- c. [Data minimisation - Ensure the data you are processing is:](#)
 - a. Adequate
 - b. Relevant
 - c. Limited to what is necessary

¹ The ICO has guidance on '[criminal offence data](#)'. Under the Data Protection Act 1998, criminal records data was covered by the 'sensitive information' guidelines.

- d. **Accuracy**
 - a. Take reasonable steps to ensure data is not incorrect or misleading
 - b. You may need to amend the data in light of new information
 - c. Take reasonable steps to correct inaccurate or misleading data
 - d. Carefully consider any challenges to the accuracy of personal data
- e. **Storage limitation**
 - a. Do not keep personal data for longer than needed
 - b. Justify any retention period
 - c. Periodically review data and anonymise or delete as appropriate
 - d. Carefully consider challenges to retention of data
 - e. Only retain data for longer periods for public interest archiving or research purposes
- f. **Integrity and confidentiality**
 - a. Ensure appropriate security is in place to protect data
 - b. Take responsibility for what you do with data and how you comply with other principles
 - c. Have appropriate measures and records in place to ensure compliance
- g. **Accountability**
 - a. Demonstrate compliance with the GDPR
 - b. Have data protection policies in place
 - c. Appoint a data protection officer
 - d. Document processing and process breaches
 - e. Carry out impact assessments for uses of personal data that are likely to result in high risk to individuals' interests

You will need to consider how to apply these principles to your own recruitment practices, but they must be adhered to and there are consequences for not doing so. [Article 83\(5\)](#) of GDPR provides for fines up to €20m or 4% of annual turnover for failure to comply with these principles so employers will want a good understanding of their responsibilities when processing personal data, including criminal records data.

Criminal record disclosure rules

The rules that apply to the disclosure of criminal records are complex. They apply both to asking applicants questions during recruitment ('self-disclosure') and to official criminal record checks (provided in England and Wales by the Disclosure and Barring Service).

This section provides the key points you need to know when recruiting.

Asking applicants to self-disclose

- The [Rehabilitation of Offenders Act 1974](#) (ROA) supports the reintegration of people with convictions by giving them legal protection from having to disclose their record after a legally determined period of living crime free. After this rehabilitation period criminal records can be [considered 'spent'](#).
- Most convictions will become spent. Once spent, the person doesn't need to disclose it when applying for most paid or voluntary jobs.
- Most jobs are covered by the ROA and, where it applies, you are not allowed to consider convictions that are spent under the Rehabilitation of Offenders Act 1974 (ROA) – it would be illegal for you to do so.
- Where the criminal record is unspent, it is generally up to the discretion of the employer whether or not to employ the person.
- For roles [exempt from the ROA](#), an employer is entitled to consider both unspent and spent convictions and cautions, but is not allowed to take into account [protected convictions and cautions](#).²

Carrying out official criminal record checks

The Disclosure and Barring Service (DBS) is responsible for issuing official [criminal record checks](#). The level of check that can be carried out for a particular role is set out in legislation.

1. For roles covered by the ROA, an employer can carry out a basic criminal record check. This contains details of unspent convictions only. An individual can apply for their own basic check, or an organisation registered with the DBS as a 'responsible organisation' can also apply, subject to the individual's consent.
2. For roles exempt from the ROA, an employer can carry out a standard or enhanced criminal record check, depending on the specific role. A standard check contains unspent and spent convictions and cautions, but not those convictions or cautions that are now [protected](#) (i.e. filtered by the DBS). An enhanced check contains the same information, but can also include other information that the police deem relevant to the role applied for – e.g. arrests or allegations that didn't result in a formal outcome. If the role involves working in 'regulated activity' with adults or children, the enhanced check can also involve a check against the adults' and/or children's barred list.

² This is known as the 'filtering' process, which is operated by the DBS when issuing standard and enhanced checks.

Current recruitment practice

Asking individuals to self-disclose

No employer has a legal obligation to ask about criminal records at application stage, but the majority still do. Unlock carried out a survey of 81 well-known, national employers' online application systems, and the findings will be published in full in autumn 2018. We analysed online application forms and recruitment policies (where available) to assess employers' attitudes and approach to recruiting people with criminal records.

The employers we analysed span eight sectors: Supermarkets; Retail; Construction; Utilities and Services; Car Manufacturers; Food and Restaurants, Communications and Leisure and Tourism. The vast majority of roles at each of the employers we surveyed would be covered by the Rehabilitation of Offenders Act 1974 - meaning employers would be under no legal obligation to ask about criminal records at any stage in the process, and in most cases a criminal record would not affect an applicant's ability to carry out the job.

Although the questions alone do not reveal an employer's attitude to recruiting people with criminal records, the quality of the questions and any guidance or support offered to applicants do provide an indication of how much thought an employer has put into recruiting this group.

Some of the key findings of our research shows that:

1. Of 78 online application forms available, almost 75% asked applicants to declare a criminal record.
2. 76% of employers who asked the question provided no guidance to applicants
3. 25% of employers had phrased the question in a way that was either unlawful or misleading
4. Three applications ended when our test applicant ticked the box declaring an unspent conviction
5. None of the construction companies we surveyed asked about criminal records at application stage.

One of the key points of this guidance is that collecting criminal records at application stage is unlikely to be necessary.

Carrying out criminal record checks

For roles that are covered by the ROA, the majority of employers do not obtain basic criminal record checks. Some of these employers will have asked individuals to self-disclose and will base their decision on this information, others will have not asked individuals to self-disclose. This is reflected in the number of basic checks that are being applied for – in 2016/17, just over 1.3 million³, which is significantly lower than the number of jobs that would be eligible for a basic check.

For roles that are exempt from the ROA, employers mostly carry out standard or enhanced criminal record checks after a job offer has been made. This is reflected in the number of these checks carried out each year – in 2016/17, there were just over 4.3 million checks issued by the DBS.⁴

³ The DBS took over full responsibility for issuing basic checks in early 2018, so there are no annual figures from the DBS. In the financial year 2016-17, Disclosure Scotland issued 1,382,250 checks to applicants in England and Wales.

⁴ The DBS issued 4,335,385 standard and enhanced checks in the financial year 2016-17.

Section 2: Ensuring compliance

From the outset of the recruitment process, you will be asking individuals to share personal data - their name, address, contact details, qualifications, work experience and skills which you'll need to enable you to contact the applicant and assess their suitability for a role.

Under the GDPR, you must consider what information is necessary at each stage of the recruitment process. This includes personal data of all kinds but you will need to consider the particular compliance requirements of collecting criminal records data at any stage in the recruitment process. To demonstrate compliance, you will need to:

1. Define the purpose of collecting criminal records data,
2. Identify a lawful basis and a condition for processing, and
3. Set out your privacy policy and ensure applicants and employees are made aware of their rights over personal information you collect.

This section explains each of these in more detail.

1. Defining the purpose of collecting criminal records data

What is your organisation's purpose in collecting criminal records data? Without a purpose, it will not be possible for most employers to identify a lawful basis. In any case, if there is no specific purpose data processing would be unfair and excessive.

There are exceptions – for example, if you are employing staff to carry out regulated activity, say in a nursery, you have a legal obligation to collect criminal records data. In that situation, the purpose and the lawful basis are closely linked. That will not be the case for most employers and, when defining your purpose, you will need to demonstrate that you have considered the following:

1. Why do you need to collect criminal records data?
2. What benefit is expected from collecting criminal records data?
3. What would be the impact of not collecting criminal records data?
4. What is the intended outcome for individuals?
5. Are you complying with other relevant laws (for example the ROA)?

It is important that the purpose has been clearly defined and that you can demonstrate a [clear and rational link](#) between the processing and the fulfilment of the purpose. The point at which data is collected will also affect whether it is necessary at that stage – for example, it is unlikely that collecting criminal records data at application stage is necessary. The collection of criminal records data must be necessary to fulfil the purpose. **If the processing is not necessary, it is not [lawful](#).**

2. Identifying a lawful basis and a condition for processing

There are six [lawful bases](#) under which you can collect personal data of any kind. You should have already identified the lawful basis for collecting applicants' personal data as part of your broader approach to data protection, but, as criminal records data is special category data, the specific lawful basis for processing criminal records should also be documented.

You may apply the same lawful basis to the collection of criminal records data, or you may identify a different basis for different data. In a very few cases, the purpose is implied in the lawful basis and it will be immediately clear whether this applies to your workplace. For example, if you are legally obligated to ask about criminal records, your purpose is 'to comply with the law' and the lawful basis is 'legal obligation'. In any case, the purpose and lawful basis should be documented and accessible to applicants.

Part 1 – Identifying a lawful basis for collecting criminal records data

The lawful bases are listed below, with some questions to help establish whether that is an appropriate lawful basis for you to use and examples of job roles where they would be appropriate.

1. Contract

Is there a clear reason why an employee contract requires collecting criminal records data?

Example: An agency providing nursing or teaching staff.

2. Legal obligation

Are you legally obliged to collect criminal records data?

Example: A school, nursery or care home, where enhanced DBS checks are required from the regulator.

3. Vital interests

Are you collecting criminal records data to save or protect someone's life?

Example: There are no workplaces where this would seem to be a suitable lawful basis for collecting criminal records data.

4. Public task

Are you collecting criminal records data as part of official tasks/functions in the public interest?

Example: Prison or police service (sworn officers only), some jobs in government departments

5. Consent

Can applicants still be considered if they refuse to answer questions on criminal records?

Example: Any employer can use this basis provided consent is genuine, but it is unlikely to be a satisfactory basis to rely on as it would require giving individuals a genuine choice as to whether they answer the question. It would also have to allow individuals to withdraw their consent.

6. Legitimate interests

Have you a legitimate interest in collecting criminal records data AND can protect the rights of the individual?

Example: Any employer can use this basis, but the purpose must be clearly defined. There are more details on this below.

Part 2 – Identifying a condition for processing criminal records data

In addition to having a lawful basis, employers who are processing criminal records data will also need to comply with Article 10 of the GDPR and identify a condition for processing. These can be found in [Schedule 1 of the DPA18](#) but most are likely to rely on Part 1. This condition is met if –

- (a) the processing is **necessary** for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection, **and**
- (b) the controller has an **appropriate policy document in place** (see paragraph 39 in Part 4 of this Schedule). (Para 1)

Meeting the condition depends on both *demonstrating that processing is necessary*, **and** *having an appropriate policy in place*.

Selecting a lawful basis and meeting the condition for processing

It is clear that most lawful bases will not be open to most employers. The ICO's [interactive tool](#) will help you select an appropriate lawful basis. We anticipate that most will rely on [legitimate interests](#) as it is the most flexible basis – but it requires work to identify and define the purpose of collecting criminal records data.

If you are relying on legitimate interests, it is recommended that you carry out a [Legitimate Interests Assessment \(LIA\)](#), a three-part test that takes into account **purpose, necessity** and **balance**. Weighing your defined purpose against necessity and balance will help you determine whether legitimate interests is a suitable lawful basis. (Note - Even if you select another lawful basis, you will need to demonstrate that collecting criminal records data is necessary and that applicant's rights are not infringed, so it is worth documenting the answers to these questions).

Documenting the LIA will help you *demonstrate that processing is necessary*. You will then need to develop an *appropriate policy* (otherwise known as a privacy policy).

1. Purpose

You will have defined your purpose using the questions on page 9. The following questions will help you consider necessity and balance.

2. Necessity

Compliance requires you to demonstrate a clear and rational link between collecting criminal records data and your stated purpose.

1. Will collecting criminal records data help you achieve your purpose?
2. Is collecting the data proportionate?
3. Can you achieve your purpose without processing the data, or by processing less data?
4. Can you achieve the purpose by another, less intrusive, means?

If the purpose can be achieved another way, processing is not necessary and therefore fails the necessity test.

3. Balance

The balance test ensures that the purpose of processing is weighed against the impact on an individual applicant.

1. Criminal records data is sensitive information; consider the applicant's reasonable expectations of what their data will be used for
2. Do your recruitment policies accurately reflect what an applicant can reasonably expect?
3. What are the likely impacts on the individual?
4. What can you put in place to minimise any negative impact on the individual?

Processing will only be necessary if the purpose of collecting criminal records data outweighs an individual applicant's right to privacy. **If the processing is not necessary, it is not compliant.**

3. Setting out your privacy policy and data subject rights

To meet the condition of processing you will need to have an [appropriate policy in place](#). An appropriate policy is also described in the legislation as a privacy policy and we use that term here as it better describes the aim of that policy – to ensure, as far as possible, the privacy of individuals whose data is being collected.

Individuals have the right to be informed about the collection and use of their personal data. **This is a key transparency requirement under the GDPR.**

Your existing privacy policy will probably cover the purpose and lawful basis for collecting various types of personal data. However, to meet the condition for processing criminal records data you must include your purpose/s for processing this data specifically, the retention period, and who it will be shared with.

Your policy on the collection, use and retention of criminal records data **must** be available to applicants at the time the information is collected. If you obtain personal data from other sources (for example from data in the public domain), you **must** provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

If you collect criminal records data as part of the recruitment process, you must have a specific privacy policy covering this.

The policy should:

- Define the purpose of processing this information and how collecting it is necessary to fulfil the purpose
- Make clear your lawful basis and condition for processing criminal records data
- Indicate how long personal data will be retained
- Provide information to applicants on their [data subject rights](#). These are:
 - o The right to be informed
 - o The right of access
 - o The right to rectification
 - o The right to erasure
 - o The right to restrict processing
 - o The right to data portability

- The right to object
- Rights related to automated decision making including profiling

Failure to provide this information will mean you have not met the 'condition for processing' requirement and the processing of criminal records data is unlikely to be compliant with Article 10 of the GDPR.

Examples of existing policies

Many employers now feature privacy policies on their website. These cover the collection of all types of personal data. These policies are generically termed 'privacy policies' but compliance with the GDPR and the DPA18 requires a privacy policy to contain the three specific elements set out on page 9: purpose, lawful basis and information on retention periods, sharing and data subject rights.

In this section we analyse two example policies, focusing specifically on the section relating to processing criminal records data. These were available online as of September 2018. In analysing these two policies, we conclude that neither are likely to be compliant. Amendments are suggested for each.

Supermarket

The extract below is from their privacy policy:

We may process information about criminal convictions if we consider it necessary for the role.

Basis for processing: This processing is necessary for us to comply with our legal obligations and in accordance with our legitimate interests (to ensure that our recruitment practices help us attract and retain the best employees).'

The supermarket asks the following question on their application form

Your offer of employment will be subject to a satisfactory disclosure from the Disclosure and Barring Service (DBS).

Failure to reveal information relating to any relevant unspent convictions could lead to withdrawal of an offer of employment. Please select to indicate 'I do not have any unspent convictions, cautions, reprimands or final warnings'. Or, if this does not apply to you, enter details of any unspent convictions, cautions, reprimands or warnings below.

1. Defining the purpose of collecting criminal records data

- The stated purpose of collecting criminal records data is to 'help us attract and retain the best employees'. It is unclear how collecting criminal records data is necessary to achieve this purpose. If the processing is not necessary, it is not compliant.
- The implication is that applicants with criminal records are not 'the best employees' – yet the available evidence from proactive employers shows that, on the contrary, they make excellent employees. In any case, it is unclear how collecting criminal records data from applicants has any effect on either attracting or retaining employees.

2. Identifying a lawful basis and a condition for processing

- It is not clear for which – if any – job roles the supermarket will process information about criminal convictions nor why it is necessary for those roles.
- It is not clear that any roles confer a legal obligation on the supermarket to collect criminal records data. It is unlikely that any supermarket roles would be exempt from the ROA and therefore this lawful basis does not apply.
- Legitimate interests could be an applicable lawful basis, but there is no Legitimate Interests Assessment and the supermarket does not specify which roles would necessitate processing of criminal records data, or why.
- It is not clear what level of DBS check the supermarket intends to carry out – they are legally only entitled to carry out a basic check.
- The question about criminal records is somewhat misleading – it implies that applicants must disclose any cautions, reprimands or warnings. In fact the supermarket is only legally entitled to ask about unspent convictions.

3. Setting out your privacy policy and data subject rights

- No information on retention periods or applicants' rights is provided.
- Applicants have no way of knowing how long their data will be retained for, or their right to have it erased.
- The absence of this information means the condition of processing is not met.

Suggested amendments

- The supermarket should ensure there is a clear and rational link between collecting criminal records data and fulfilment of their purpose.
- They should also clarify for which roles it is 'necessary' to collect criminal records data, and why.
- It is unlikely that they will be able to justify asking all applicants at the application stage.
- They should also make clear which jobs, if any, they are carrying out criminal record checks for and under what legislation or regulation.
- The supermarket should provide a privacy policy specifically in relation to their collection of criminal records data and explain to applicants what their rights are, data retention periods and whether and how data will be shared.
- The supermarket should consider whether it is necessary to ask about criminal records at application stage.
- The supermarket should ensure that, if they ask, they ask only about unspent convictions, and that applicants know they will only be asked to complete a basic criminal record check.

DIY retailer

The extract below is from their privacy policy:

We may collect information about your criminal convictions history if it is appropriate given the nature of the role and where the law allows us to do so. This will usually be where such processing is necessary to carry out our legal obligations or exercise rights in connection with employment, and provided we do so in line with [parent company's] Policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your vital interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

The retailer asks the following question on their application form:

Do you have an unspent criminal conviction for any of the following offenses? No/ Murder/ Manslaughter/ Theft / Fraud / Sex Offence including Paedophilia / Grievous Bodily Harm/ Actual Bodily Harm

1. Defining the purpose of collecting criminal records data

- The policy does not explain the purpose of collecting criminal records data, so it is not clear what the purpose is, nor how collecting this information is necessary. If the processing is not necessary, it is not compliant.

2. Identifying a lawful basis and a condition for processing

- It is not clear for what roles the retailer considers it 'appropriate' to carry out criminal record checks, nor is it clear how an applicant could find out.
- A DIY retailer is unlikely to have m/any roles that are exempt from the ROA, so 'legal obligation' is unlikely to be an applicable lawful basis. The phrase '...rights in connection with employment' implies legitimate interests but it is not clear what the legitimate interests are, nor how the employer's rights are exercised by collecting this data.
- The policy references vital interests. It is unlikely that collecting criminal records from applicants would be a matter of life or death, or why that information would be used in a situation where an employee was 'not capable of giving [their] consent'. It is unlikely that any employer can rely on vital interests as a lawful basis on which to collect criminal records data from applicants.
- The policy suggests the employer will consider information in the public domain. In general, information about criminal convictions in the public domain is from news media, is not always reliable and usually remains accessible long after a conviction is spent (and therefore must legally be ignored).

3. Setting out your privacy policy and data subject rights

- No information on data subjects' rights is included, it is not clear how long data will be retained, nor how applicants can request erasure.
- The absence of this information means the condition of processing is not met.

Suggested amendments

- The retailer should clarify the purpose of collecting criminal records data, explain why it is necessary and identify the lawful basis for doing so.
- When making reference to the parent company's policy, the employer should provide a link to that policy and reference the specific parts that apply.
- Data in the public domain should only be processed by an employer if they can reasonably show that the data was 'manifestly made public by the data subject'. ([DPA18: Schedule 1, Part 3, Para 32](#)). The use of personal social media and news reports of criminal cases is unlikely to be 'manifestly made public by the data subject'. The employer should make explicit what information they will gather and how it will be used, and consider why they are using this and how they can uphold data subjects' rights around access, erasure, and accuracy if they use it. Using this information is also likely to be unfair if individuals are not aware of it, potentially breaching Principle a.
- The retailer should consider whether it is necessary to ask about criminal records at application stage.
- The retailer should state whether they intend to carry out a criminal record check. If they do not, they should consider whether it is necessary to ask applicants to self-disclose.

Section 3: If and when to ask

In most cases, there is [no legal obligation](#) for an employer to ask about criminal records. Asking about criminal records creates legal obligations under the GDPR and the DPA18. So, if you currently ask about criminal records, ask “why do we do this?” Being clear about your purpose will help you to assess whether processing fulfils it or not.

If you decide you need to ask at any stage, you must provide a [clear and rational link](#) to the lawful basis for asking and to your privacy policy – that includes the retention periods and who data will be shared with. This should be documented in plain language and be transparent, concise and accessible. We recommend following the steps in section 2 above, and considering the points below to decide when it is necessary to ask.

Asking about criminal records on application forms

Asking all applicants to disclose at application stage is **unlikely to meet the necessity test** as it is neither a specific nor targeted means of collecting criminal records data.

- There are usually many more applications than there are positions – unsuccessful applicants will have unnecessarily had to disclose their criminal record.
- Most legitimate interests in collecting this data could be met by collecting less data – for example, by only asking the applicant offered the role.

If you use online systems that currently require the disclosure of criminal records before an application can be submitted, their privacy policy must provide the lawful basis and purpose of collecting this at application stage. Data controllers are responsible for demonstrating compliance so where an employer [contracts a 3rd party](#) to host online application portals that collect criminal records data from every applicant, the employer is responsible for ensuring only necessary information is collected.

Automated decision making

As noted on pages 12-13, the GDPR provides several data subject rights, including rights related to [automated decision making including profiling](#). This means you are accountable for safeguarding against the risk of a potentially damaging decision being taken without any human intervention (the balance test).

The GDPR applies to all automated individual decision-making and profiling. Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.

Notwithstanding the point made above – “Asking all applicants to disclose at application stage is **unlikely to meet the necessity test**” - where online application forms ask about criminal records, you will need to review the process to ensure it complies with Article 22 of the GDPR.

Where online systems make automated decisions based on an applicant's disclosure, you must ensure that the decision making is:

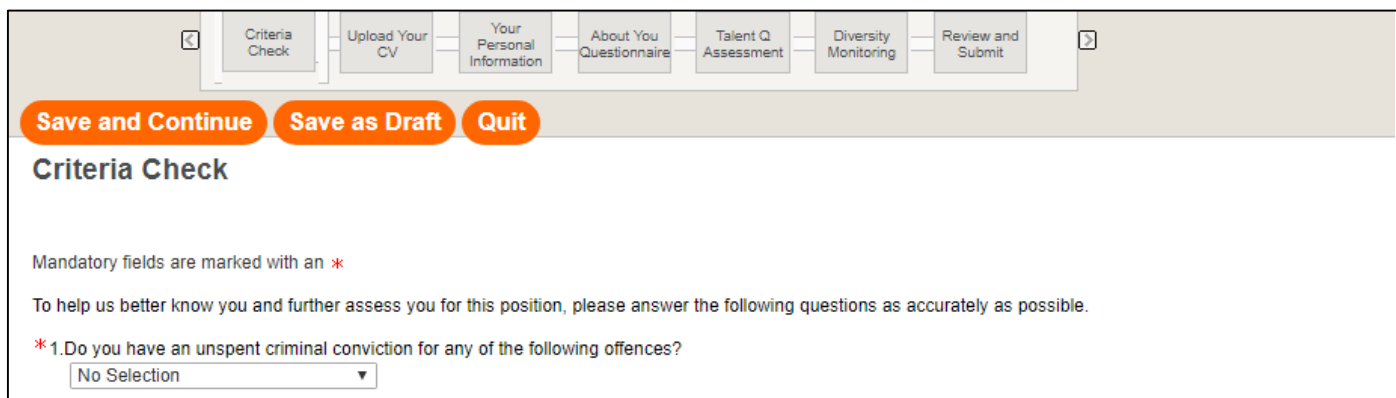
- necessary for the entry into or performance of a contract; or
- authorised by law applicable to the controller; or
- based on the individual's explicit consent.

You must also ensure that you:

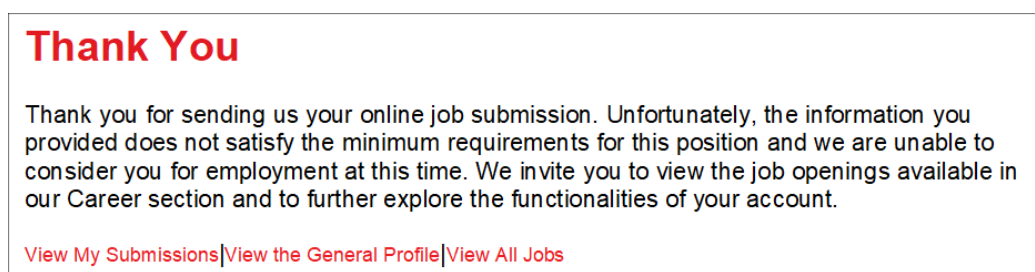
- give individuals information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision;
- carry out regular checks to make sure that your systems are working as intended.

We know of some application systems that make automated decisions to decline applicants based on criminal records disclosure although it is not clear how widespread this practice is. The GDPR and the DPA18 requires controllers to *demonstrate* compliance with the data protection principles, including transparency about how and why employee information is processed, and employees' rights to access, amend or erase their personal data.

Below is an example of an automated decision process that does not comply with Article 22 of the GDPR.



On ticking the box to indicate 'yes, I have an unspent criminal conviction' the applicant is taken to this screen:



The decision is fully automated, applicants are not asked for consent and are not provided with information about the automated decision making or how to challenge the decision. Automated decision making of this type does not comply with Article 22 of the GDPR.

Asking at job offer stage

For most jobs you are not allowed to consider convictions that are [spent](#) under the Rehabilitation of Offenders Act 1974 (ROA) and therefore you should not ask about these at any stage unless you are legally obliged to. It would be unlawful under the ROA and a breach of the GDPR to ask about spent convictions. In addition, unspent convictions do not legally prevent people from working in most jobs, so you should consider whether you need to ask about these at all at job offer stage.

If you are certain that you need to ask applicants about criminal records at this stage, you should consider what to ask and how to collect that information, and formulate a [policy](#) that can be shared with applicants. The lawful basis for doing so must be available to applicants from the outset and the process for disclosing and making decisions should be clearly set out. Remember that you must ensure that you only use applicants' data in ways that they might 'reasonably expect'. If you plan to carry out searches of material in the public domain – news sites, social media – you should explain how this fits with your lawful basis and ensure that processing does not infringe applicants' data subject rights.

Written information, whether official or provided by an individual, can be difficult to put into context. Give applicants the opportunity to explain the surrounding circumstances in person to address any concerns you might have. Don't limit a discussion about their criminal record just to the behaviour that led to their offence. Instead, focus most on what the applicant has done since; encourage them to discuss their rehabilitation and the positive steps they've subsequently taken.

You should also establish your organisation's approach to the following question: Is it 'reasonable' to deny an otherwise qualified applicant employment because of a criminal record that may be years old, or not relevant to the job, or may have occurred in particular circumstances? If it is reasonable, document these reasons in your policy so that applicants can make informed decisions – and your company's time is not wasted.

Carrying out official criminal record checks

The GDPR does not prevent you carrying out basic DBS criminal record checks. The DPA18 includes a provision which allows checks where it is 'necessary for the purposes of performing or exercising employment law obligations or rights'. The key word is **necessary**. As with asking applicants to self-disclose, the purpose of carrying out criminal record checks must be defined and you must demonstrate the necessity of carrying out checks. You must also identify the lawful basis under which checks are carried out.

Some application forms ask applicants to consent to a basic check. The GDPR has heightened the consent threshold which needs to be 'explicit and freely given'. Making it a condition of employment that employees consent to a basic check is not true consent. In addition, if data is processed on the basis of consent, processing must halt at the point that an individual withdraws consent. There is an imbalance of power between an applicant and employer, so if you select consent as a lawful basis, it must be genuinely consensual. If it is not possible for an individual to withdraw consent and still have their application considered, consent is not an appropriate lawful basis.

Some employers can be legally obliged to carry out criminal record checks. The [Rehabilitation of Offenders Act 1974 \(Exceptions\) Order 1975](#) sets out where standard or enhanced criminal record checks can be done for specified roles or professions. You'll need to be certain that you're legally entitled to obtain criminal records data about your employees and that you're sure about the level of criminal record check which can be undertaken. If you were to carry out an ineligible criminal record check (for example doing a [standard or enhanced check](#) for a role which would only be eligible for a [basic check](#)), then you could be in breach of [data protection principles](#):

- Principle (a) - "Lawfulness, fairness and transparency"
- Principle (c) - "Data minimisation"

Knowingly requesting a level of DBS check for a post *not* listed in the Exceptions Order is a criminal offence under Part V, section 123 of the Police Act.

It is also a criminal offence under section 184 of Data Protection 2018 to require a person to provide or give a relevant record in connection with recruitment or ongoing employment – that means it is an offence to require applicants or employees to exercise their subject access rights to obtain information from the police.

Section 4: Conclusion

The full implications of the GDPR are still being embedded, but it is clear that data controllers must comply with data protection law. This guidance makes it clear what employers should be doing, and we expect that individuals will look to challenge those organisations that operate policies and practices that do not comply.

To ensure compliance, employers must demonstrate that processing criminal records data is **necessary** at whatever stage they decide to collect it. If processing is not necessary, it is not compliant.

Key points in this guidance are that:

1. Collecting criminal records at application stage is unlikely to be necessary and therefore in breach of the GDPR and the DPA18
2. Collecting criminal records at *any* stage must be justified by a link between purpose and processing.
3. You must identify a lawful basis for processing AND meet a condition of processing
4. Applicants have data subject rights that must be upheld
5. Explaining how you will uphold applicants' rights is essential to GDPR compliance

We suggest that employers no longer ask about criminal records at application stage – and seriously consider whether they need to ask at all.

Employers should join Ban the Box

The considerations in this guidance link strongly to our work to encourage companies to join the [Ban the Box](#) campaign. Ban the Box calls on UK employers to create a fair opportunity for people with convictions to compete for jobs by removing the tick box from application forms and asking about criminal convictions later in the recruitment process. Ban the Box calls on UK employers to create a fair opportunity for people with convictions to compete for jobs by removing the tick box from application forms and asking about criminal convictions later in the recruitment process.

Unlock was a co-founder of the campaign, and has supported the work of Business in the Community, who lead the campaign, since its launch in 2013. We promote the campaign as part of our [fair access to employment](#) project and our work to encourage fair chance recruitment practices by employers in the UK. Behind the scenes, we work with employers to help them put the principles of the campaign into practice, using our knowledge and experience of working with both individuals who have convictions as well as employers who are actively looking to improve their recruitment policies and practices so they can recruit the best candidates regardless of their background.

What's wrong with the box?

- It makes it difficult for applicants to get past the initial sift as it is often used to deselect applicants
- There is no opportunity to contextualize or to explain
- People deselect themselves from applying, so employers miss out on potential applicants
- It can lead to discrimination against people with protected characteristics – for example BAME people are disproportionately affected by criminal records
- No employer legally has to ask about criminal records at application stage

Banning the box means you can consider criminal records at a more appropriate stage in the recruitment process, giving people with convictions a fair opportunity to compete for jobs. Far too often we hear from people who are unable to get past the application part of a recruitment process simply because they have to tick 'yes' to the questions about convictions. For employers, the end goal has to be to try and find the best person for the job, and with over 11 million people in the UK with a criminal record, banning the box is a key step towards this goal.

Too often, employers overlook skills, experience and qualifications if an applicant declares they have a criminal record. Employers should Ban the Box as the first step to recruiting the best candidates for their jobs. However, we encourage you to go further and consider whether you need to ask about criminal records at all. Most jobs do not legally require applicants to disclose at any stage and there is no evidence that employees with a criminal record are any less reliable, hardworking or trustworthy than employees without. In fact, an increasing body of evidence shows that employees with criminal records are at least as good, if not better employees.

Annex A - Checklist

There are a number of recommendations in this guidance. This checklist summarises the key things that you should make sure you have in place *before* processing criminal records data.

Have you...

1. Defined the purpose of collecting criminal records data?
2. Identified a lawful basis for collecting criminal records data?
3. Identified a condition for processing criminal records data?
4. Set out why the processing is necessary to fulfil the purpose?
5. Developed a privacy policy that explains, with specific reference to criminal records data;
 - a. The purpose of processing
 - b. The lawful basis for processing
 - c. Why processing is necessary
 - d. How long data will be retained
6. Provided information to applicants, with specific reference to processing criminal records data, on their rights?
 - a. The right to be informed
 - b. The right of access
 - c. The right to rectification
 - d. The right to erasure
 - e. The right to restrict processing
 - f. The right to data portability
 - g. The right to object
 - h. Rights related to automated decision making including profiling
7. Removed questions about criminal records from the application stage?

More information and useful resources

This guidance was first published in September 2018. The latest version is available online at recruit.unlock.org.uk/dataprotection

This guidance is part of the practical guidance we provide via [Recruit!](https://recruit.unlock.org.uk) – our website providing advice and support for employers on recruiting people with convictions and dealing with criminal records fairly.

We are grateful for the advice and support that we have received from the Information Commissioner's Office in producing this guidance. Links to their guidance are embedded in the document and more information is available on their [website](https://ico.org.uk). There is also a [useful briefing](#) produced by Nacro on data protection and the use of criminal offence data.

For further advice about this guidance, please contact us: recruit@unlock.org.uk.

Published by Unlock © 2018. All rights reserved.

Written by Rachel Tynan and Christopher Stacey.

Unless otherwise indicated, no part of this publication may be stored in a retrievable system or reproduced in any form without prior written permission from Unlock.

Unlock and the authors are not legally trained or qualified. Any information or guidance given in this publication should not be taken as a substitute for professional legal advice. Unlock is unable to accept liability for any loss or damage or inconvenience arising as a consequence of the use of any information provided in this guidance.

Unlock is a registered charity no. 1079046 and a company limited by guarantee, registered in England and Wales no. 3791535.

Registered office: Maidstone Community Support Centre, 39-48 Marsham Street, Maidstone, Kent, ME14 1HH
Telephone: 01622 230705
Email: admin@unlock.org.uk
Twitter: [@unlockcharity](https://twitter.com/unlockcharity)
Website: www.unlock.org.uk