Unlock response

ICO survey - Processing of personal data relating to criminal convictions

About Unlock

Unlock is an independent, award-winning national charity that provides a voice and support for people with convictions who are facing stigma and obstacles because of their criminal record, often long after they have served their sentence. Our focus is predominantly on people in England and Wales.

Firstly, **we help people.** We provide information, advice and support to people with convictions to help them to overcome the stigma of their criminal record. This includes running an information site which has over 1 million visitors a year, and a confidential peer-run helpline that helps around 8,000 a year. This work is charitably funded; we do not deliver government-contracted services. We help practitioners support people with convictions by providing criminal record disclosure training. We support employers, universities and others to develop and implement fair and inclusive policies and procedures that enable the recruitment of people with convictions and that treat people with criminal records fairly.

Secondly, **we advocate for change**. Every year we hear from thousands of people who are unnecessarily held back in life because of their criminal record. We work at policy level to address systemic and structural issues. We listen to and consult with people with criminal records, undertake research and produce evidence-based reports to inform policy makers and the public. We challenge bad practice, influence attitudes and speak truth to power. We co-founded and support the Ban the Box campaign and we are pushing to wipe DBS checks clean of old/minor criminal records. We have a track record of constructive engagement with government, the DBS and employers in working towards a fairer and more inclusive approach.

We provide advice and support to employers, universities, insurers, housing providers and others on the relevant law and best practice when processing criminal offence data. We challenge unfair and/or unlawful practice and work to influence legal and cultural change so that law-abiding people with criminal records can move on positively with their lives.

This response to the ICO's consultation on processing Article 10 data draws primarily on our experience of working with data controllers,_and in particular the guidance on GDPR that we published in October 2018, but also highlights the impact of unnecessary and disproportionate processing of criminal offence data.

Overview

Requests for Article 10 data in relation to a job, university or housing application creates worry on the part of applicants. Questions are not always clearly phrased and information about what will happen with the information is often scarce. Disclosure of a criminal record can significantly affect the outcome of a decision and being refused housing or employment, car insurance or a place at university, can have life changing consequences. For example, more than half of employers say they would discriminate against an applicant who disclosed a criminal record.

The ICO's detailed guidance on processing special category data emphasised the need to treat this type of data with greater care because collecting and using it is more likely to interfere with an individual's fundamental rights or open someone up to discrimination. That guidance indicated that data about criminal allegations or convictions may raise similar issues, albeit covered by different rules. We would expect the ICO's detailed guidance on processing Article 10 data to include the same emphasis on treating this data with care due to the potential for interference in fundamental rights and the risk of discrimination.

The ICO's guidance on processing Article 10 data should be sufficiently emphatic on the need to demonstrate the purpose and necessity of processing this data. That processing should be "necessary" is inherent in the requirement to identify an Article 6 lawful basis and Article 10 schedule condition.

There can sometimes be a legal obligation on employers recruiting for certain professions and occupations to check a candidate's criminal record. Around 75% of large employers collect Article 10 data at the point of application. Processing of Article 10 data is now so commonplace that the question of necessity is rarely considered. Controllers need clear guidance on how to assess this in light of data protection requirements. Necessity will be fact sensitive and it is likely that detailed guidance for different sectors or functions will be needed.

Requests for Article 10 data are often based on assumptions and bias rather than demonstrated necessity or a clear purpose. The ICO should be mindful of inadvertently reinforcing bias in its guidance on the collection of Article 10 data or other communications. For example, the promotion of the Article 10 survey included the following: '*Organisations may process personal data relating to criminal convictions and offences…for many reasons. For example, to… assess people's suitability for employment…* '

A small number of jobs legally oblige an employer to process Article 10 data, but the vast majority do not. Nonetheless, most employers do collect this and – in our experience – the majority do not have protocols in place to assess suitability beyond the simple collection of 'yes/no' responses to a question about unspent convictions. In guidance and communications, the ICO should be alive to the risk of inadvertently approving the collection of Article 10 data without properly interrogating the necessity of doing so.

This should also be reflected in internal guidance used within the ICO and in the way decisions are communicated. Following a recent complaint to the ICO regarding a trade body's processing of Article 10 data, a case officer's response included the following paragraph:

'In forming our view on the matter we took into account that membership of a particular professional body, such as [redacted], is likely to be indicative of someone who is reputable and trustworthy, and its members should, therefore, be able to demonstrate these characteristics.'

This reveals an underlying assumption that the processing of Article 10 data is necessary if a controller wishes to test the reputability and/or trustworthiness of a data subject_– as if disclosure of criminal offence data automatically calls into question reputability and/or trustworthiness. Taken to its logical conclusion, this assumption would mean that any controller could demonstrate the necessity of processing Article 10 data, which calls into question the need to have special protections applied at all._As the UK's independent body set up to uphold information rights, the ICO should be objective about the value of any data. People with criminal records have the same data subject rights as those without and have the same expectation that controllers will be accountable for processing their data.

Question 4: DBS/Disclosure Scotland checks

The lack of clarity around the correct level of DBS/Disclosure Scotland checks is of particular concern and not adequately covered, in our view, by existing guidance from the ICO or the DBS. Employers requesting higher level checks than a post is legally eligible for ("ineligible checks") pose a particularly difficult problem for job seekers. Although the DBS provide written guidance and tools for checking eligibility, employers can find it difficult to determine the correct level.

Employers are not legally obliged to state whether they will carry out a criminal record check or what level they will apply for, nor is it standard practice to do so. The DBS Code of Practice requires Registered Bodies and those in receipt of Update Service information to ensure applicants are notified in advance of the requirement for a disclosure and to have a policy on the recruitment of people with criminal records. However, employers in receipt of update service information will be entitled to carry out higher level checks. Most employers will never recruit for posts eligible for higher level checks, and the Code of Practice is not explicit about their responsibilities.

For employers, there are legal, regulatory and reputational risks associated with requesting an ineligible check.

- Violating the Rehabilitation of Offenders Act and the Police Act: Section 123 of the Police Act 1997 makes it an offence to knowingly request an ineligible check. The maximum penalty is six months in prison or an unlimited fine. However, the complexity of the law around disclosure makes it difficult to demonstrate an employer 'knowingly made a false statement' and, to date. there have been no prosecutions for this offence.

- Breach of data protection law: Using information in breach of the law is, in itself, a data protection violation. Obtaining an ineligible check is a breach of the Rehabilitation of Offenders Act as well as the Police Act, so processing of this information would be unlawful. Employers found to be in breach of the GDPR and/or Data Protection Act 2018 can be subject to enforcement action or financial penalties.
- Breach of an individual's data subject rights: Where an ineligible check is carried out, an individual has the right, under Articles 79 and 82 of the GDPR, to bring proceedings to court if they believe their information rights have been infringed and can be awarded damages.

In addition, data protection principle (c) requires organisations to ensure that the personal data they are processing is adequate, relevant and limited to what is necessary. Where a role is covered by the Rehabilitation of Offenders Act, processing data on cautions and spent convictions (disclosed via an ineligible higher level check) is neither proportionate nor necessary.

In practice, there is little risk to employers who attempt to carry out ineligible checks. Most applicants will be unaware that the check is ineligible, and those who are aware will often be reluctant to raise it with an employer for fear of identifying themselves as a person with a conviction. The only recourse available to an applicant is to agree to the check and then raise a concern with the DBS.

We would encourage the ICO to include clear guidance on data protection obligations when requesting DBS/Disclosure Scotland checks, in particular in relation to issues around in eligible checks, and consider how to advise individuals on whether their data subject rights have been compromised.

Question 6: data protection requirements

Understanding of data protection requirements around Article 10 data is likely to vary across sectors and between controllers. Identification of an Article 6 lawful basis and an Article 10 schedule condition depends on the purpose of processing and some purposes lend themselves more easily to particular schedule conditions – for example employment or insurance. Processing of Article 10 data by universities, housing providers, membership organisations or trade bodies requires careful consideration of Article 10 conditions in particular, and we would recommend that specific guidance is produced for processing by these types of organisations. In October 2019 Unlock published 'Developing a fair approach to applicants with criminal records: A toolkit for higher education providers'. This toolkit sets out the data protection requirements of processing Article 10 data for admissions purposes. We are aware that the ICO has produced guidance for higher education providers but there are no plans to publish it.

The use of "Consent" in both Article 6 and para 29 of Schedule 1 to the DPA is of concern. Consent is rarely used in an employment context, as the limited role of consent has been made clear in other guidance. Consent is, however, relied on by housing providers, trade bodies and membership organisations and higher education providers to process Article 10 data. The concerns about the use of consent in relation to employment are similarly live in these contexts. The power imbalance between an individual applying to university or for housing or for membership to a global trade body is no less significant than that between an individual and an employer. Clarity on the role of consent in non-employment contexts is needed.

Controllers would also benefit from clarity around a handful of other schedule conditions. In particular, the following substantial public interest conditions: Preventing or detecting unlawful acts, Protecting the public against dishonesty etc. Safeguarding of children and of individuals at risk. The function of Article 10 data in meeting these objectives is far from obvious, yet these conditions are frequently relied upon by controllers who process Article 10 data for non-employment purposes – seemingly because they refer to crime, dishonesty and safety, rather than because the processing is genuinely meeting these objectives.

Clarity about the scope of data protection requirements would be welcomed. The GDPR read with s11(2) of the DPA covers a wide range of Article 10 data including allegations of offences, conviction and sentencing. Controllers should be made aware that criminal offence data includes not only criminal record checks (via DBS) but also unverified information via self-disclosure on application forms or at interview, via reference requests or third parties, or informally through internet searches or word of mouth.

Controllers frequently obtain Article 10 data from internet searches or from other members of the organisation and use this to make decisions about recruitment or retention. This is rarely covered explicitly in appropriate policy documents and the management of information obtained or shared on electronic devices is not referenced. We have examples of staff sharing information on corporate systems, which potentially engages the issues raised in *Wm Morrisons Supermarkets Plc v Various Claimants [2018] EWCA Civ 2339*

Controllers sometimes request Article 10 data from referees, particularly in relation to employment. Referees – who would be processors in that instance - should be aware of their data protection obligations when providing Article 10 data.

Where Article 10 data is collected but not verified, the necessity of the data is questionable and we would like to see clear guidance on the processing of unverified Article 10 data. Not only is unverified information of limited utility, controllers cannot be sure when information should be deleted (for example when convictions become spent or protected) without certainty over dates.

Other areas

In October 2018, Unlock published 'Asking the question - Guidance for employers on the GDPR, data protection and the processing of criminal records data in recruitment'. With support and input from the ICO, this guidance was published in response 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).

At various points in this response, we have recommended the ICO publish clear guidance. We would extend that recommendation to ensuring that the issues covered in our guidance for employers are communicated via the ICO to employers – the ICO is in a unique position to be able to ensure that employers (and other controllers) awareness and understanding of the data protection requirements for processing Article 10 data.

More information

Written	February 2020
Contact	Rachel Tynan | Policy and practice lead, Unlock
Address	Maidstone Community Support Centre 39-48 Marsham Street Maidstone Kent ME14 1HH
Web	www.unlock.org.uk | @unlockcharity