GDPR and immigration requirements: how to fulfil both

Samar Shams explains how to comply with the General Data Protection Regulation (GDPR) when hiring migrant workers

Samar Shams is head of immigration at Downs Solicitors

'There is no requirement, from an immigration perspective, for an employer to retain data submitted in support of an individual's visa application. The privacy notice should therefore state that the organisation will not retain the data after successful completion of the visa application process.'

Immigration requirements prompt special consideration under the UK's data protection regime. The data categories, data retention requirements and international transfers involved in immigration require particular compliance measures under the GDPR and the Data Protection Act 2018 (DPA). This article examines how the GDPR affects three key areas: right-to-work checks, visa applications and the resident labour market test (RLMT).

Right-to-work checks

Lawful basis

The need to comply with a legal obligation is an appropriate lawful basis for right-to-work checks. It is contrary to the Immigration, Asylum and Nationality Act 2006 to employ an illegal worker.

There is no positive obligation on employers to perform the specified document checks: the right-to-work checks set out in the *Prevention of Illegal Working* guidance only serve to establish a statutory defence from penalty. However, a specific requirement is not needed for legal obligation to be the lawful basis for processing. It is sufficient that the overall purpose of processing right-to-work data is to comply with the clear legal obligation not to employ illegal workers and that job candidates can foresee that the prohibition on illegal working applies to them.

Individuals might present biometric residence permit cards and passports including fingerprints as right-to-work documentation. The biometric nature of the data means that it is special category data under the GDPR. A person's religion is also special category data and is noted on some passports. Therefore, the employer must identify a further condition or justification for processing the data.

Article 9(2) of the GDPR sets out the acceptable conditions. One is that the processing is necessary for carrying out employment law obligations and is authorised by law. The GDPR does not define employment law. Until further guidance is available, it is reasonable to rely on the employment law condition when checking right-to-work documents.

Privacy notice

General GDPR requirements on giving notice to individuals will apply. For example, the employer should provide a privacy notice at the time of collecting the information and identifying the lawful basis for processing.

In addition, the privacy notice must cite at least one condition justifying the processing of biometric data and data on religion, such as its being necessary for carrying out employment law obligations. The notice must state that the employer will retain the right-to-work documentation for the duration of employment plus two years and that it may share the information with Home Office officials and legal advisers.

When informing individuals of their rights, note that there is no right to erasure or data portability and no right to object since legal obligation is the lawful basis for processing right-to-work data.

Systems

The accountability principle requires businesses to be able to demonstrate

their compliance with the GDPR. It is therefore important to design systems and policies to abide by key data protection principles such as purpose limitation, data minimisation, storage limitation and security. The systems appropriate for the particular organisation will depend on a number of factors, including size.

Checking the right-to-work documents specified by the Home Office establishes a defence against civil penalties for employing illegal workers, but the specified documents do not cover all those with a right to work in the UK. Several categories of individuals have the right to work without having documentation on the Home Office lists. For example, EU nationals' direct family members are not required to hold documentation. Another example is those with the right of abode, such as Mr Baker in *Baker v Abellio London Ltd* [2017] (see 'Windrush and the right to work' by Jarmila Entezari and Sejal Raja, *ELJ*190 (May 2018), p10).

As the lawful basis is the legal obligation not to employ illegal workers, a business may request documentation beyond that specified as establishing a statutory defence against civil penalty. However, employers should consider the purpose limitation and data minimisation requirements and only request and store the minimum documentation required to establish the individual's right to work in the UK. They should also implement systems for destroying right-to-work documentation two years after the end of the relevant employment.

It is also important to document these policies and procedures.

As certain right-to-work documentation includes biometric data, a data protection impact assessment (DPIA) may be required. A DPIA includes defining the process, assessing its necessity, identifying risks and determining additional measures to mitigate risks. DPIA templates are available on the Information Commissioner's Office (ICO) website.

As certain right-to-work documentation includes biometric data, a data protection impact assessment may be required.

Visa applications

Lawful basis

Legal obligation is an appropriate lawful basis for processing data to facilitate visa applications. The Immigration Rules include provisions on leave to enter and leave to remain in the UK, the requirements of the various visa categories and the general grounds for refusing applications.

The Immigration Rules have a quasi-legal status. Parliamentary approval of the rules is by negative resolution (whereby draft rules laid before Parliament automatically become law without debate unless there is an objection from either House). However, the GDPR states at Recital 41 that a legislative measure:

> ... does not necessarily require a legislative act adopted by a parliament... [although it] should be clear and precise and its application should be foreseeable to persons subject to it.

The Immigration Rules clearly require applicants to provide personal data, including information about children, biometrics and criminality. Migrants should foresee that the Immigration Rules will apply to them when making visa applications. Therefore, the rules constitute a legislative measure setting out legal obligations.

As with right-to-work checks, visa applications involve special category data including biometrics and data on religion which might appear in a passport. The employer must therefore identify a condition under Art 9(2) of the GDPR to justify processing. The condition that the processing is necessary for carrying out employment law obligations is again likely to apply here.

UK visa application forms request information on criminal history. Certain applications require the police in countries where the applicant has been resident to certify a clear criminal record. Criminal data is not considered special category data under the GDPR but, as with biometric information, processing requires a condition or justification beyond the lawful basis. Under Art 10 of the GDPR, the processing must be authorised by law and provide for data safeguards. In the absence of case law or other guidance to the contrary, employers can rely on the DPA provision allowing for the processing of criminal data necessary to perform obligations under employment law (Sch 1 Pt 1, para 1).

Privacy notice

As with right-to-work checks, the employer should give a clearly worded privacy notice when it collects the information for a visa application.

The notice should identify obtaining a visa as the purpose of the data processing. It should also identify the legal obligation to comply with requirements in the Immigration Rules on entry clearance and leave to remain as the lawful basis for processing. The notice should further state that performing obligations under employment law is the condition justifying the processing of biometric, religious and criminal data.

There is no requirement, from an immigration perspective, for an employer to retain data submitted in support of an individual's visa application. The notice should therefore state that the organisation will not retain the data after successful completion of the visa application process. However, it is a good idea for the individual to retain a copy for their records, to ensure future submissions are consistent.

The privacy notice should also include the employer's details and inform individuals of their rights. As legal obligation is the lawful basis for processing the data, there is no right to erasure, data portability or right to object.

The ICO recommends providing children with tailored privacy notices:

> ... so that they are able to understand what will happen to their personal data, and what rights they have.

However, it is not clear how an employer would comply in the context of visa applications. Perhaps this area of data protection practice will develop and become clearer.

Systems

If a business is supporting employees with their visa applications and

sending their data to third parties such as translators, it will need contracts in place with those third parties. The contract must include specific details such as the subject matter, duration and purpose of the processing and the type of personal data. Specific terms on the scope of the processing and the third party's safeguards are also required. The EU Commission or ICO may draft standard clauses in future.

When supporting employees and job candidates with visa applications, employers also often process information about the individual's family members, including children. The GDPR requires heightened protection when children are data subjects. The ICO suggests it is best practice to use a DPIA to assess and mitigate risks to children when processing their data. As discussed above, an employer is also required to undertake a DPIA when handling biometric data.

When dealing with visa applications, GDPR restrictions on transfers of personal data outside the EU might apply. For example, the employer might need to send an individual's data to overseas counsel or an overseas courier company.

The European Commission may condone transfers to specified third countries if it is satisfied that their data protection is adequate. No specific authorisation will be required for such transfers. The Commission has determined that protection is adequate in a handful of countries, including New Zealand, Switzerland, Argentina and Israel, and made more limited adequacy determinations about the US and Canada.

Alternatively, adequate safeguards for overseas transfers may be provided in various other ways, including an agreement between public authorities, the binding rules of a corporate group, and standard clauses adopted or approved by the Commission. The European Commission has published standard clauses for transfers of data outside the EU; these predate the GDPR and so may be revised.

Resident labour market test

Lawful basis

A UK employer wishing to sponsor a non-EEA migrant to work in the UK is often required to fulfil the RLMT to ensure that there are no settled UK workers available to fill the role. RLMT requirements include advertising the role and retaining shortlisted candidates' applications.

A lawful basis for retaining such applications is the employer's legitimate interest in complying with requirements on immigration and protecting the resident labour market. However, an employer can only rely on this lawful basis after conducting a legitimate interests assessment (LIA).

An LIA involves first identifying the interest: consider why the organisation wants to process the data as well as any benefits to the public. Immigration compliance and protection of the resident labour market both benefit the wider public. Next, an LIA requires the organisation to consider whether the processing is necessary to further that interest. The Home Office has set out the RLMT requirements in official published guidance, which shows that it has deemed the processing necessary to achieving the objectives.

The final stage of an LIA is to conduct a balancing test, by considering the impact of the data processing on the individual and whether that overrides your interest. Factors include whether the data is sensitive or private. Much of the data included in job applications is not private and is often available on LinkedIn or elsewhere on the internet. However, some data is sensitive or private, for example contact details. The organisation should therefore consider whether it can adopt any safeguards, such as anonymisation, pseudonymisation or encryption, to strengthen the balancing test in favour of processing.

Completing the LIA should enable employers to demonstrate that it is proportionate to process and retain shortlisted candidates' application information. The interest in immigration compliance and protection of the resident labour market is a compelling, societal one and little or no harm comes to the individual, particularly when the organisation uses safeguards.

Alternatively, the lawful basis for retaining these job applications might be to comply with a legal obligation because fulfilling the RLMT is a requirement in the Immigration Rules. However, processing of the information according to RLMT requirements would have to be foreseeable by a regular job applicant and it is not clear that it would be. Therefore, it is probably best not to rely on this basis for RLMT data processing, although this may change as GDPR jurisprudence develops.

The GDPR requires heightened protection when children are data subjects.

Privacy notice

Employers must notify shortlisted applicants that they are relying on legitimate interests as the lawful basis for processing. The privacy notice should explain that the purpose of the processing and the legitimate interests are immigration compliance and protecting the resident labour market. It should state that the organisation will retain the individual's application for up to one year after it stops sponsoring a migrant who might fill the vacancy. The notice should also include the organisation's details and inform individuals of their rights. As the lawful basis is legitimate interests, the right to data portability does not apply.

Systems

Employers should document having undertaken an LIA. They should also implement a system for destroying the documentation either one year after sponsorship of the relevant employee ends or after a compliance officer has examined and approved the documentation, whichever is earlier. This will fulfil sponsor record-keeping duties as well as GDPR requirements. ■

Baker v Abellio London Ltd [2017] UKEAT/0250/16