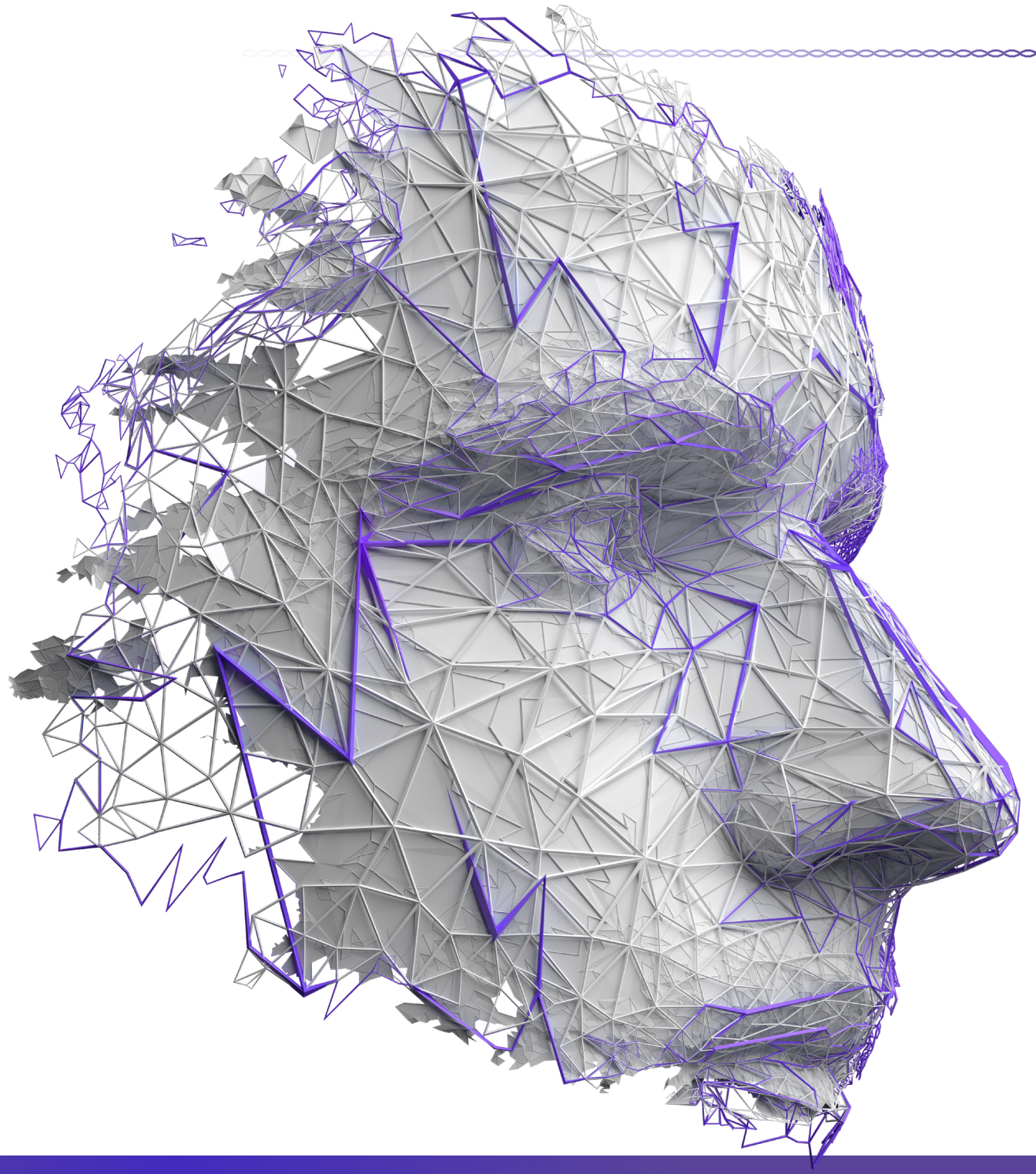
ICO'S NEW GUIDANCE EASES DIGITAL RECRUITMENT CHALLENGES

Gemserv®

A Talan Company

Since the spread of COVID-19 in early 2020, employers have seen drastic changes to work practices. Office behaviours have changed, and digital and remote forms of hiring have evolved with them. Within this context, on 12th December 2023 the Information Commissioner's Office (ICO) issued draft guidance on data protection practices in relation to recruitment and selection, and opened a consultation until 5th March 2024.

The draft guidance is aimed at employers, recruitment agencies, head-hunters and other organisations involved in candidate hiring. There is a particular focus on the challenges of sourcing and researching candidates online and using AI technologies within interviews and assessments. Hiring organisations, particularly those using such recruitment processes, should consider a review in light of the ICO's new draft guidance and data protection law. They should also consider responding to the consultation. This article walks through the provisions of the ICO's draft guidance for organisations at various stages of the recruitment and selection process.



WHAT ARE THE REQUIREMENTS FOR ORGANISATIONS TO CONSIDER?

The ICO's draft guidance provides an outline of the legislative obligations (which it calls 'musts' to comply with) and examples of best practice (which organisations 'should' comply with) across several recent digital recruiting practices. It's worth noting that organisations that don't follow the 'shoulds' may need to be prepare an answer if investigated. The following sections cover the provisions of the ICO's draft guidance and outline the requirements for hiring organisations at various stages of the recruitment and selection process.

POSTING AN OPENING

According to Statista[1], almost half of job applications now stem from an employer or recruiter's online advertisement. This is an opportunity for the hiring firm to show candidates how they will process personal data during recruitment. As the ICO explains, if employers use a recruitment agency, the recruiter is also responsible for "advertising the vacancy" and providing transparency about any data handling. In both circumstances, advertisers will need to provide a link to a Privacy Notice in a job advert, application form, or page on an application tracking system. As the ICO details, this notice needs to provide potential recruits with information including "your purposes for processing; how long you will keep their information; and who you will share it with".

Under the ICO's draft guidance, organisations must also provide transparency about:

- the use of any information sourced on candidates from social media – including candidates' public profiles, if applicable. This is imperative to ensure that recruits are aware, and reasonably expect, that any information on their social media pages may be used to evaluate their suitability for positions.
- the use of any "solely automated" decision-making or profiling, including "meaningful details about the logic involved and the significance and likely consequences for the candidate". This could apply, for example, where an organisation uses an AI tool to score or sort candidates based on their suitability for positions. It involves explaining the 'how, what and why' of the use of personal data by the AI system; any risks of inaccuracy or biased decisions for individuals; and mitigations in place for these risks.

[1]Statista. (2023, Oct 4). Online and social media recruiting - Statistics & facts. Retrieved from https://www.statista.com/topics/2727/online-recruiting/#topicOverview.

Potential recruits should also know their rights before they begin an application. When outlining a data subject's rights per the UK GDPR, the employer should describe any procedures for candidates to "explain or challenge any information that may not be accurate" during the interview process. In the case of solely automated decisions made during the hiring process, this should also include their right to obtain "human intervention" to express their point of view.

SCREENING AND PRE-SELECTION

Once the applications begin to roll in, HR teams and hiring managers may find themselves sifting through and researching candidates to make the right decision. In accordance with the 'data minimisation' principle under Article 5 of the UK GDPR, data collection must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". When using digital application tracking systems, the ICO explains that one method of achieving this could be to "tailor your application forms to ensure that candidates only provide the information you need". This will prevent unnecessary information about a candidate from being handled. In our experience, methods to avoid the collection of unnecessary data could involve, for example, a "blind CVs" policy. In this method, Human Resources (HR) remove candidate photos or names from their applications before forwarding their CV to the hiring manager to reduce the potential for bias.

Online research into candidates is also increasingly used by recruiters. 57% of hiring firms reported in a Statista survey that they have at some point chosen not to hire a candidate based on content found on social media[2]. When researching candidates, the ICO states that hiring firms and recruiters must only "collect information that is relevant and necessary for recruitment" and not use data in ways the candidate would not reasonably expect.

Here, context is very important. For example, whilst according to the ICO it "may be reasonable to manually search for information using recruitment-based social media platforms" (such as LinkedIn), the content of a recruit's personal social media posts (such as on Instagram) are unlikely to be relevant or necessary to assess their suitability for a role, except for positions involving contact with children or other vulnerable individuals.

Organisations should also avoid 'inferring' information about a candidate based on content they have posted online. The ICO states that this would involve both an unfair and potentially inaccurate processing of data.

[2]Statista. (2023, Oct 4). Online and social media recruiting - Statistics & facts. Retrieved from https://www.statista.com/topics/2727/online-recruiting/#topicOverview.

BACKGROUND CHECKS

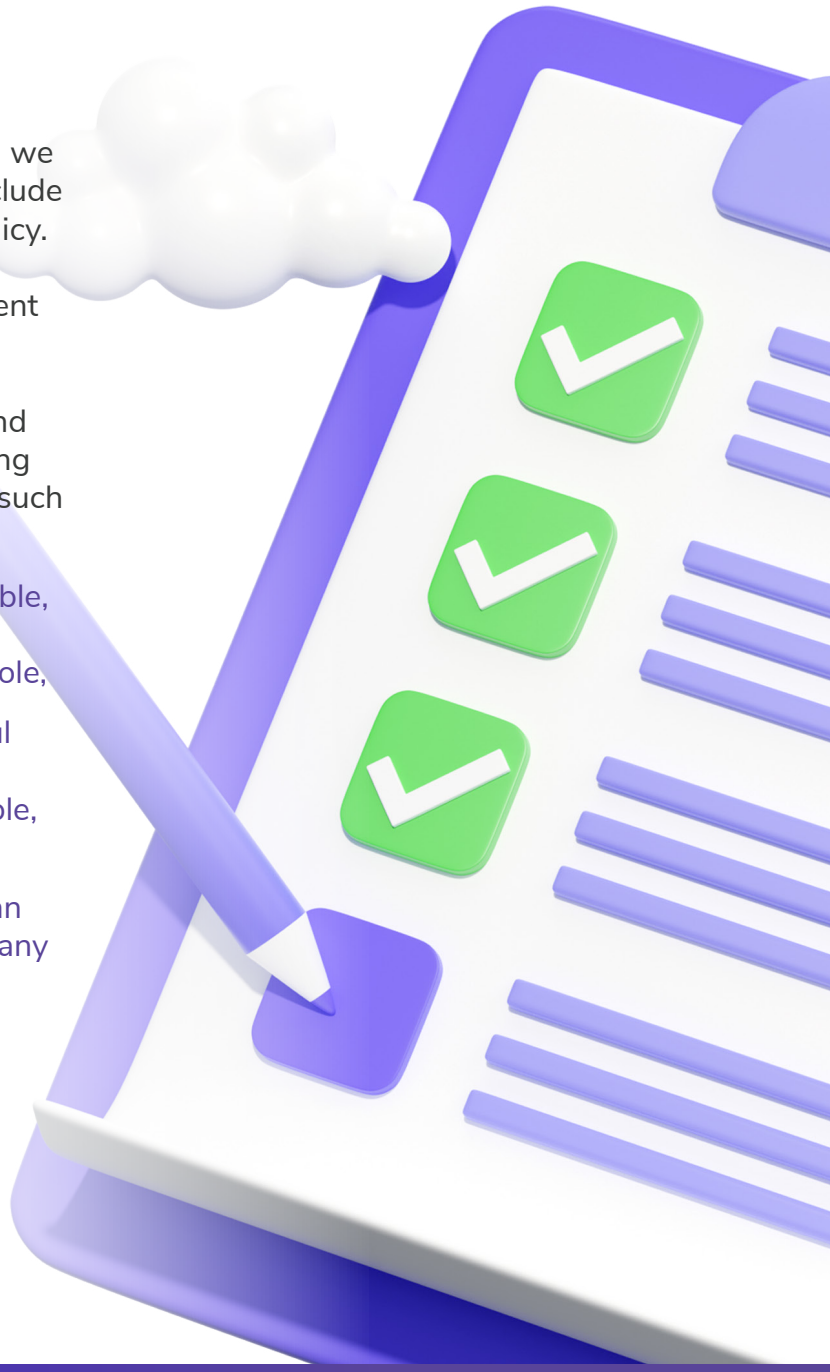
Depending on the role, recruiting organisations may conduct more detailed background checks into candidates. The ICO draft guidance provides that such checks – such as into a candidate's political beliefs, credit history or criminal convictions – should only be performed where hiring firms:

- "are under a legal obligation (e.g. to perform right to work checks)" or
- "can identify significant and particular risks to the employer, clients, customers, or others"

In the first case, for roles such as teachers and solicitors listed under the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975, employers can conduct detailed checks. For all other roles, according to the ICO, the legality of checks will depend on the nature of the role and should involve consideration of risks to working with vulnerable people, national security or the "disclosure of trade secrets or other commercially sensitive information".

To avoid collecting data through background checks unless necessary, we find that an effective measure can include introducing a Background Checks Policy. Employers would train both HR staff and hiring managers to use a consistent approach towards the appropriate collection of background information. To ensure such checks are relevant and proportionate for roles and avoid losing candidates for unnecessary reasons, such a policy should:

- cover the type of vetting permissible, depending on the legality of such checks and the sensitivity of the role,
- limit such checks to the successful candidate alone or later in the recruitment process where possible, and
- cover providing candidates with an opportunity to explain or contest any findings that the checks find.



INTERVIEWS AND ASSESSMENT

For candidates making it to the interview stage, the modern hiring process increasingly includes interviews conducted across conferencing platforms such as Zoom or Microsoft Teams.

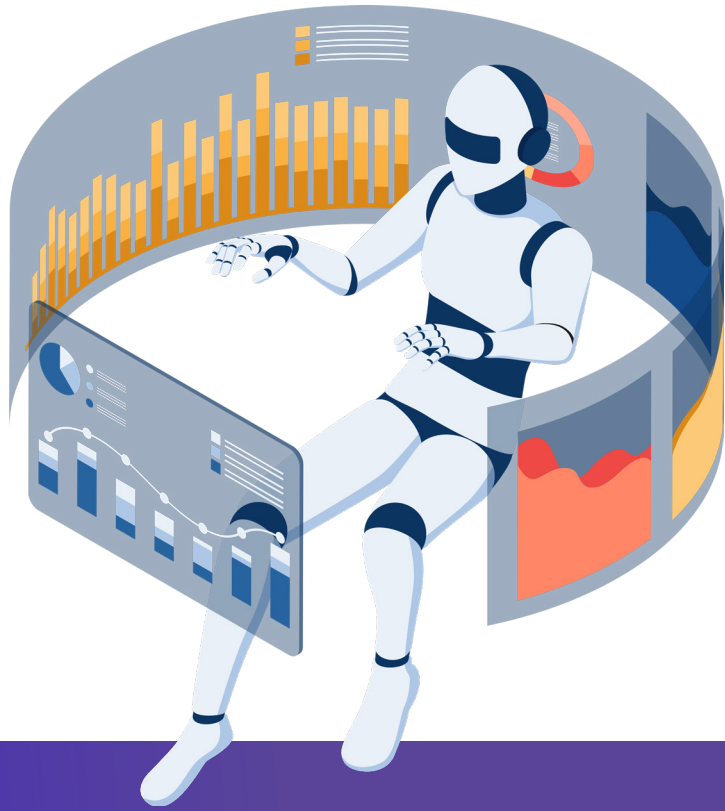
Some platforms also offer the potential for employees to submit video-recorded applications or personal statements. In this context, the ICO advises on data minimisation methods that can be used, including to liaise with applicants attending interviews online to avoid "processing unnecessary information" through the video camera, such as data on third party family members or religious beliefs.

Alongside interviews, hiring firms with large volumes of applications have also turned to deploying artificial intelligence (AI) to rank and sort candidates. The ICO advises that using AI to make decisions about candidates carries the risk of inaccuracy. Errors can include the individual's CV mischaracterised as having no right to work in the UK, or biases, such as an AI-assisted video interview discriminating against candidates with speech impediments. Consequently, Article 22 of the UK GDPR restricts the use of "automated decision-making", using AI systems that "produces legal effects" or "similarly significantly affects" an individual.

Using an AI tool to make decisions about whether to progress with a candidate is likely to create such a "similarly significant" effect. As a result, the ICO's draft guidance states that recruiting organisations must conduct a data protection impact assessment (DPIA) for the use of AI in recruitment as it is "likely to result in a high risk to the rights and freedoms of candidates".

This can help organisations consider whether the use of AI in particular assessments or stages of recruitment is "necessary and proportionate" to the nature of the role and volume of applications. It can also support in evaluating any potentially biased or inaccurate outcomes and considering proper mitigations. From our work with organisations deploying AI, such measures could include:

- To avoid the risk of making a "wholly automated" decision, introducing a means for human intervention in the assessment process, as the ICO recommends. In a recruitment context, this could involve both an AI-assessed test and an in-person interview forming part of a candidate's cumulative score.
- To avoid the risk of biased or adverse effects for individuals, maintaining the ability to "monitor" and "correct inaccuracies and minimise errors". This can be achieved through data tracking to discover patterns, such as if there's an overly high rate of unsuccessful applicants from minority ethnic backgrounds.



POST-OFFER AND ONBOARDING

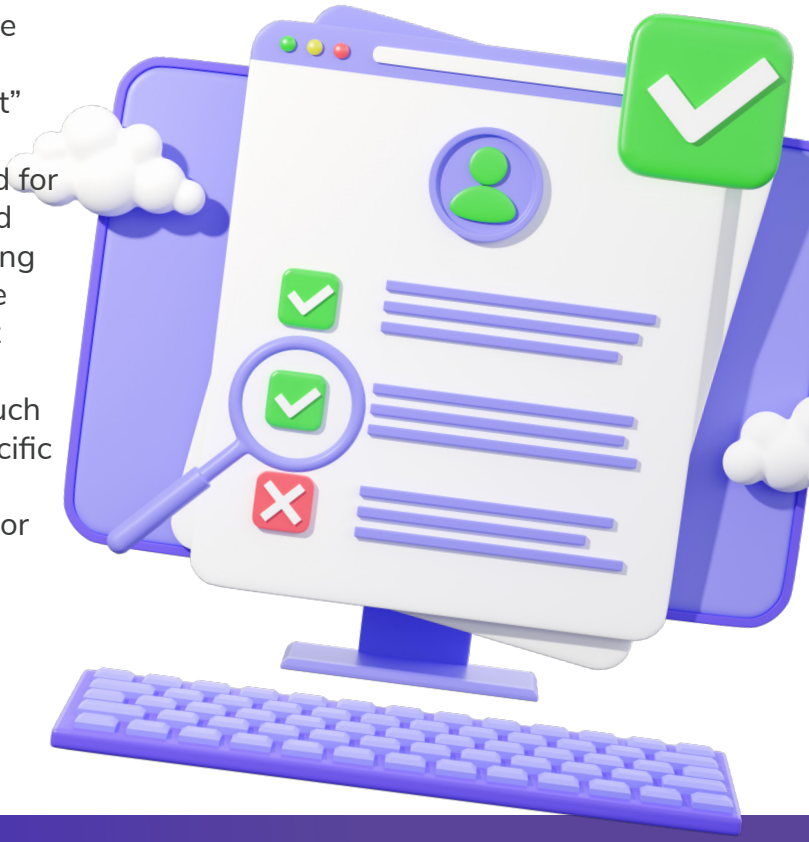
Once a suitable applicant has been selected and an offer been made, employers will need to consider which data generated during the recruitment process is reasonable to retain. From our observations, a successful candidate's records, including right to work evidence, their references and other documents, will typically become part of their employment file. This is so a firm can take steps "prior to entering into" as well as "the performance of" their employment contract.

For unsuccessful candidates, however, the ICO explains there are a few circumstances where records may be kept, such as:

- Retaining contact details of candidates, such as to offer them future positions.
- Retaining demographic information on candidates for statistical analysis of the success rate of candidates from different backgrounds (which should be anonymised where possible).
- Retaining assessment data, such as the interview notes and assessment scores, for "statutory limitation periods", such as to defend against claims of discrimination from unsuccessful candidates. Such periods are set by law, such as by the UK's Limitation Act 1980.

For each of these, employers must establish a legal basis under Article 6 of the UK GDPR. Examples include if the processing is "necessary for compliance with a legal obligation" or "necessary for the purposes of a legitimate interest" as identified by the organisation. This purpose, as well as the retention period for the candidate's file, must be maintained in an organisation's Record of Processing Activities. We often see that firms have a practice of retaining CVs to reach out to unsuccessful candidates for future positions. However, the suitability of such an approach is likely to be context-specific to the position, and more relevant for large organisations with high turnover or specialist positions.

As the ICO writes, recruitment agencies may have other purposes for the retention of records, such as to record if they will support an unsuccessful candidate for further roles. In these circumstances, such firms may want to consider the retention of records needed to comply with their obligations under the Conduct of Employment Agencies and Employment Businesses Regulations 2003.



FINAL THOUGHTS

The draft update to the ICO's guidance is very timely. By providing a clarification on obligations arising throughout the increasingly digitalised recruitment process, it provides a useful set of guidelines for the era of widespread remote and AI-assisted hiring in the UK. We would recommend that all recruiters read the draft guidance and consider responding to the consultation to ensure that the final guidance is as useful as possible.

After the consultation closes in March, the ICO expects to issue its final guidance and keep it under review. In a changing area, and with the potential for the Data Protection and Digital Information Bill (DPDI) to amend obligations around automated decision-making and data protection impact assessments later this year, organisations should use the draft guidance to trigger and maintain an evaluation of their recruitment practices.

AUTHOR

Kaveh Cope-Lahooti
CIPM, LLM, MBCS, Principal Consultant (Cybersecurity & Privacy)

kaveh.cope-lahooti@gemserv.com
BD@gemserv.com