

LABOUR AND THE LAW

A JAMES NJERI & Co. ADVOCATES NEWSLETTER



EMPLOYMENT BACKGROUND CHECKS ARE SUBJECT TO DATA PROTECTION REQUIREMENTS

Employment background checks are carried out by employers to screen potential employees or candidates and to verify the information that they have provided during the recruitment process.

For Employers, it is essential to screen the new hire to ensure that they are suitable for the role. But what happens when an employee is successful in the interview and then fails the background check, which ends up in them losing the job opportunity? Should an employee be informed of the findings of the background check?

This was the question posed in a complaint to the Data Protection Commissioner recently in ***ODPC Complaint No. 0586 of 2023. Harrison (Complainant) V Faulu Microfinance Bank Limited (Respondent)***.

The Office of the Data Protection Commissioner is a regulatory office mandated with regulating the processing of personal data. Part of their core mandate is to receive complaints from individuals who believe that their data has not been processed in accordance with the law.

Background

The brief facts are that the Complainant attended an interview at the Respondent's Company to fill a vacant position. He was invited for two interviews, on the 15th and 23rd March 2023, where he emerged as a successful candidate and was informed of the same. On the 28th of March 2023, he received a consent form requesting to carry out background checks on him and afterward, he was issued with an official letter of intent of employment subject to verifications being conducted. On 15th April, 2023 the Respondent informed the Complainant that upon conducting background checks, it would not be proceeding to offer him employment.



James WaNjeri
Advocate



Christina Njeri
Advocate

EMPLOYMENT BACKGROUND CHECKS ARE SUBJECT TO DATA PROTECTION REQUIREMENTS

The background check generated an adverse report on the character of the Complainant due to a discovery that he was the subject of an active criminal case. However, this information was not given to him and he was only informed verbally that there was an adverse report touching on his character.

Upon being informed of this development, the complainant requested for a copy of the data that the respondent relied upon to arrive at its finding. The Respondent refused to share the information with him, indicating that it was private. The issue was, therefore, whether the Complainant was entitled to receive the adverse report and whether it constituted the Complainant's personal data.

Legal Basis

Article 31 of the Constitution of Kenya guarantees every person's right to privacy. This right protects against someone's private information being unnecessarily revealed. The Data Protection Act (DPA) then provides safeguards to secure this right.

For starters, personal data is any information about a living person that can identify them, either directly or indirectly, and the individual whose data you seek is identified as a "**data subject**". The law protects data subjects by guaranteeing their right to access their personal data or to have it corrected if it is inaccurate. To access the personal data, the DPA requires you to obtain the data subject's consent e.g. when conducting employee background checks.

In this particular case, the Complainant, upon signing and executing the consent form, consented not only to the use of his personal data by the Respondent but also for the Respondent to collect his personal data indirectly from other sources. The Consent form also provided for the right of the Complainant to request and receive a copy of the personal data processed.

In their response to the complaint, the Respondent indicated that the Complainant had been accused before the Magistrate's Court of the offence of conspiracy to defraud contrary to section 317 of the Penal Code. In its defence, they stated that this case was public knowledge and personally known to him, and therefore, they had no physical report to issue to him.

The Data Protection Commissioner found that under Section 26 of the Data Protection Act, data subjects have the right to access their personal data and to be informed about how it is being used. Further, under the Data Protection General Regulations (2021), organizations that process data have an obligation to provide data subjects with access to their personal data upon request. The Complainant had been denied access to the data that emanated after the background checks were conducted. He argued that the processed data had been used against his selection and it was, therefore in his best interest to access a copy of the data to enable him to follow up for resolution. He was informed that he could not access a copy of the data or the source as it was private information.

The decision of the Office of The Data Protection Commissioner (ODPC) was that the complainant's right to access his personal data had been violated. First, the complainant had a legitimate expectation that he could receive the information upon request. This was clearly provided for in the consent form issued by the Respondent Employer.

EMPLOYMENT BACKGROUND CHECKS ARE SUBJECT TO DATA PROTECTION REQUIREMENTS

Secondly, the information in the report contained information that identified the Complainant by name. Under the DPA, such an identifier constitutes personal data. Having established that any information relating to the Complainant constituted personal data, the Data Protection Commissioner made a finding that the Right to Access is absolute and they therefore directed the Respondent to issue the background report to the complainant.

Conclusion

So, what is the lesson here for employers? First, it is fundamental that the Employer ensures that they have a vibrant and rigorous Data Protection Policy that governs how they collect, process, use and store data touching on their employees and the candidates they seek to recruit. This is one way to ensure they operate within the law and avoid unnecessary legal risks.

Secondly, data subjects have specific rights under data protection laws. These rights include the right to access their personal data and to be informed about how it will be used. The days of withholding information are long gone and it is critical that organisations embrace a culture shift in that respect.

Interviewees, in particular, should be aware that they have the right to access data resulting from background checks conducted during the interview process. This is especially significant if that information determines whether they obtain employment. The DPA gives the candidate the right to correct any information used in making a decision against them if it is wrong information. Before the background check is done, the interviewee should first give their consent for their data to be obtained and processed. Interviewees should establish what the recruitment process entails to establish at what point the recruitment formally ends and the job starts.

To consult us on employment and data protection matters, send us an email on legal@jnadvocates.com

The contents of this newsletter do not constitute legal advice and are provided for general information purposes only.

James Njeri and Company Advocates
Landmark Plaza, 13th Floor,
Argwings Kodhek Rd. Nairobi

Tel: 0719494083

Email: legal@jnadvocates.com

