

White Collar and Investigations Practice

November 15, 2019

DATA CONSIDERATIONS IN EMPLOYEE INVESTIGATIONS IN INDIA

PROLOGUE

There has been a surge in internal and employee-related investigations at an organizational level over the last couple of years. This may correspond to an increase in statutory requirements and disclosures pertaining to certain allegations, or concerns arising out of internal complaints from employees, external complaints from stakeholders, whistleblower complaints or even organization-driven investigations. Updating policies, handbooks and codes of conduct along with training employees at all levels have become top priority. It is not just the famous cases which hit newspaper headlines due to involvement of CXO's; internal investigations have become inevitable.

As is the case with most investigations, internal employee investigations are data-heavy and involve collection, handling, storing and processing a large amount of employee data. Often, organizations engage external advisors including lawyers, auditors and forensic experts to assist in the investigation process. Further, as in the case of multi-national corporations (MNCs) in India, overseas group entities may also be involved in overseeing or assisting in the process. Hence, the process may not be exclusively between the employer organization and employee, but other entities are also added to the manifest to ensure compliance across jurisdictions based on their presence.

A BORDERLESS WORLD

Organizational work-related data in custody with an employee may not be confined to an office computer anymore but may also be accessed or stored on an employee's mobile, tablet or laptop, whether organization owned or not, and in more recent cases even wearables such as smart watches and IoT driven home devices. It is not uncommon to notice individuals checking their work emails on their Fitbit at the gym over the weekend!

In a seamless and borderless world of data, managing data privacy concerns of the employee and statutory compliances under law, including where foreign law compliances may be triggered in case of MNCs, is a challenge. In this piece, we attempt at dissecting some of the major considerations relating to employee data that an organization should tackle when conducting employee investigations.

IT'S ALL IN THE DATA

Data protection in India is currently governed by the *Information Technology Act, 2000 ("IT Act")* and the *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011* issued thereunder ("Data Protection Rules"). The IT Act and Data Protection Rules contain provisions on confidentiality, privacy and security for information stored in a computer resource and protect sensitive personal data or information collected from individuals by corporates.

The Indian data protection rules broadly protect two categories of data pertaining to individuals, 'personal data' and 'sensitive personal data'. Personal data relates to an individual, which either directly or indirectly in combination with other information, may be capable of identifying such a person. Personal data of an individual could include a person's name, contact details, address, identifier etc. Sensitive personal data on the other hand consists of specific items of data, namely passwords, financial information, physical, physiological and mental health condition, sexual orientation, medical records and history, and biometric information.

As such, there are no specific compliances under the Indian data protection rules for collection, handling or storage of an individual's personal data although in case of unauthorized sharing or misuse of such information causing harm to the individual, penalties may be applicable in the form of imprisonment and fine. On the other hand, there are certain compliances applicable to entities that collect, handle or store sensitive personal data of individuals, and organizations would need to adhere to such compliances when conducting internal investigations. One may note here that such compliances may not need to be complied with in case of furnishing employees' sensitive personal data as part of court or enforcement agencies' proceedings or investigations.

WHEN DO ORGANIZATIONS NEED TO SIT UP?

Typically, employee data relating to work and the workplace should not contain their sensitive personal data, but it is not uncommon for employee's financial information (such as bank account numbers in case of financial investigation), biometrics for attendance record details, health records in case of medical situations etc. to be involved and collected as part of the investigation process. In cases wherein the employee's sensitive personal data is collected, handled or stored by the employer organization (or any third party as mentioned above, on the employer's behalf), certain compliances should be adhered to. In cases, wherein organizations engage external advisors including lawyers and forensic experts to assist in the investigation process, or in the case group entities are involved in the handling of employee sensitive data, such third parties if located in India may also need to comply with some of the below compliances.

Major compliances to be undertaken by the orga

1. Providing the employee with adequate notice and disclosure that their sensitive personal data may be collected

Research Papers

Structuring Platform Investments in India For Foreign Investors

March 31, 2025

India's Oil & Gas Sector— at a Glance?

March 27, 2025

Artificial Intelligence in Healthcare

March 27, 2025

Research Articles

2025 Watchlist: Life Sciences Sector India

April 04, 2025

Re-Evaluating Press Note 3 Of 2020: Should India's Land Borders Still Define Foreign Investment Boundaries?

February 04, 2025

INDIA 2025: The Emerging Powerhouse for Private Equity and M&A Deals

January 15, 2025

Audio

CCI's Deal Value Test

February 22, 2025

Securities Market Regulator's Continued Quest Against "Unfiltered" Financial Advice

December 18, 2024

Digital Lending - Part 1 - What's New with NBFC P2Ps

November 19, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

Vyapak Desai speaking on the danger of deepfakes | Legally Speaking with Tarun Nangia | NewsX

- for the purpose of an organization-driven investigation. Essentially, the employee should have knowledge of (a) the fact that sensitive personal data is being collected; (b) the purpose for the collection of such data; (c) the intended recipients of such data; and (d) the name and address of third parties collecting/retaining/processing such data (if applicable).
- Obtaining an explicit consent from the employee if the employee's sensitive personal data is contemplated to be collected for the investigation.
 - Having a privacy policy in place, which should contain clear and accessible statements of the practices and policies of the organization collecting the sensitive personal data, the type of sensitive personal data collected, the purpose of collection and usage of the sensitive personal data, onward disclosures, if any, and the security practices and procedures implemented in relation to the sensitive personal data of the employee.
 - Giving the employee the right to access, review and correct the sensitive personal data of theirs provided.
 - Appointment of a grievance officer that should address any grievances of the employee in relation to the handling of their sensitive personal data as part of the investigation.
 - If sensitive personal data of the employee is sought to be transferred to a third party such as an external service provider or a group entity of the employer organization, then specific consent should be obtained from the employee, and the employer organization should ensure that the recipient entity adheres to the same level of data protection as adhered to by the employer organization as required under the Indian data protection rules.

WHOSE DEVICE IS IT ANYWAY?

Organization owned devices

Organization owned devices such as mobiles, tablets and laptops are typically owned by the employer organization and provided to employees on a temporary basis or during the course of their employment with the employer. Such devices are considered property of the organization and not personal property of the employee. Hence, organizations when conducting an investigation requiring access to such devices, may not require a specific consent from the employee vis-a-vis accessing and inspecting the device.

To close the loop on this, should the organization owned device not contain any sensitive personal data of the employee but only work related, then the organization need not require a consent from the employee to access and inspect such device as part of its investigation.

Bring Your Own Device

In recent times, it is common for organizations to allow employees to use their personal devices for work related communications, as per a 'bring your own device' (BYOD) policy. This policy essentially allows, for instance, an employee to use her/his mobile phone, tablet or laptop to carry out work-related functions and work-related communications. Hence, organization and work-related data would sit on the employee's personal devices in such cases.

Such devices used under a BYOD policy should be construed as the personal property of the individual and not property of the organization, in spite of it containing organization and work-related data. In such case, the IT Act provides that if any person accesses a computer system or network of another person, or downloads, copies or extracts any data from such computer system or network without permission of the owner, then such person may be penalized and be made to pay compensation to the affected person. To avoid attracting this penal provision, the organization would need the employee's consent to inspect the employee's device as part of its investigation.

TAKE-AWAYS:

As an investigation begins, obtaining data of custodians is the natural starting point. In such a situation, the legal team assisted by the forensic team will, no doubt, arrive at a bridge where they will need to obtain data from a device where sensitive personal data is likely to be stored. In such a situation, the company's policies, manual and/or employee handbook are usually the first port of call to understand the rights of the company and its investigative team.

It would be pertinent to note that the organization would most probably (prior to and even during the course of the investigation) already be collecting, handling and storing sensitive personal data of its employees for instance bank account details to pay salaries or medical records data as part of its recruitment process requirements. The organization may, thus, already be adhering to the compliances under the data protection rules. In such cases, incremental but tailor-made changes may be made at an organization level to ensure that the compliances undertaken cover the organization's investigation as well, for instance updating the employee privacy policy, manual or handbook and taking necessary employee consents.

However, the overall approach of the organization should be looked at holistically including from a reputational perspective. It is vital for an organization to have its policies and employee documentation updated and in check prior to commencing an internal investigation. It would also be important for organizations to word their policies, manuals, handbooks, documentation and consents appropriately so as to not cause ambiguity between an employee and itself. It is critical to ensure that these manuals/handbooks build in adequate safeguards and proper approvals and consents from employees with respect to not only obtaining data stored on company owned devices/personal devices but also processing, imaging and transferring them in any part of the world, including to third party service providers or overseas group entities, if required.

When foreign elements come into play, such as collection of data from an employee that may be a citizen of a foreign country, or when a foreign organization comes into the mix, then consulting foreign counsel on compliances should also be carried out, so as to not violate foreign law.

DISCLAIMER

The contents of this hotline should not be construed as legal opinion. View detailed disclaimer.

This Hotline provides general information existing at the time of preparation. The Hotline is intended as a news update and Nishith Desai Associates neither assumes nor accepts any responsibility for any loss arising to any person acting or refraining from acting as a result of any material contained in this Hotline. It is recommended that professional advice be taken based on the specific facts and circumstances. This Hotline does not substitute the need to refer to the original pronouncements.

This is not a Spam mail. You have received this mail because you have either requested for it or someone must have suggested your name. Since India has no anti-spamming law, we refer to the US directive, which states that a mail cannot be considered Spam if it contains the sender's contact information, which this mail does. In case this mail doesn't concern you, please unsubscribe from mailing list.