DSCI
PRIVACY
LEADERSHIP FORUM

PRIVACY AT THE WORKPLACE

A Practical Guide to Ethical Employee Data Management

Author

- Abha Tiwari

Contributor

- Shivangi Malhotra

Abstract

This document intends to provide guidelines on personal data life cycle management, with respect to the data collected pre, during, or post the association of an individual with their workplace. This is a working document and is subject to review and future amendments and it is in no way intended to serve as legal advice.

Disclaimer

Foreword

Privacy, as a discipline, has moved forward substantially over the last few years. More so, in terms of the consciousness that is being witnessed across the globe, vis-à-vis treatment being meted out to personal information. Multiple dimensions, facets and nuances of the subject are coming to the fore which is nudging the ecosystem in a direction where Privacy considerations have started taking centre stage.

Organizations are expected to diligently think through, formulate and execute their data handling practices. Several digital economies across the world have been making great strides when it comes to strategizing their Data Protection regimes. Comprehensive legislations anchored on the principles of transparency, accountability and demonstrability are being enacted and entities which are custodians of personal information are working towards streamlining their practices to foster consumer trust and build confidence with the regulatory machinery.

While a good comprehension has started kicking in with regard to the fundamental principles of Privacy, several organizations are still figuring out the most optimal way for carrying out the operationalization of these principles. Lot of organizations are just getting started with their respective journeys. DSCI has been working along with the industry to build those capacities and capabilities that could enable Privacy implementation.

The DSCI Privacy Leadership Forum, an industry effort in this regard, has been set up to lay emphasis on the on ground practical challenges and impediments. The forum, structured in the form of Special Interest Groups (SIGs), is being driven by Privacy leaders and heads of leading organizations, who have pooled in their invaluable experiences, perspectives, and sheer hard work, to produce work products with the hope that the ecosystem finds these documents fruitful and is able to leverage them in the best possible fashion.

These work products are intended to be living documents that keep getting refined and enriched with the critical and constructive feedback from the readers of the said documents.

DSCI would like to express its heartfelt thanks to the members of the SIGs and the Privacy fraternity for their steadfast support to the discipline.

Vinayak Godse
CEO, Data Security Council of India

Table of Contents

1 Introduction

This document is intended to shed light on the emerging trends and concerns with regard to 'Right to Privacy' in the context of employment or within a workplace. References to 'employees' in the scope of this document and recommendations relating to them are not limited to traditional employer-employee relationships. Other types of economically beneficial engagements, such as those involving gig workers or freelance service providers connected via digital platforms have also been discussed. The central principle remains that the workers, in exchange for economic benefit in terms of compensation, trade in their skill/labour to add value to the organization. The productivity of the worker directly impacts the profit accrued by the organization for its stakeholders. In doing so, they are expected to provide information to be collected, stored, and processed by their organization.

Privacy, as understood in the common parlance, is of four types: (i) informational privacy, concerned with establishing regulations that govern the processing of personal information, (ii) bodily privacy, focussed on a person's physical being and any invasion thereof, (iii) territorial privacy, dealing with restrictions on the ability to intrude another individual's space, and (iv) communications privacy, encompassing protection of the means of correspondence, including postal mail, telephone conversations, email, and other means of communication.

Informational privacy of workers in the workspace can be understood as the control exercised by workers over the data/information collected and processed about them by the organization. This includes the processing of personally identifiable data collected through the range of technologies, tools, and equipment deployed in the process of value creation. The degree of control that can be exercised by a worker directly implies the 'rights' and 'protections' that are granted or guaranteed to the worker.

The privacy rights of employees and the business interests of the organization may prove to be contradictory or conflicting in certain scenarios due to the following factors:

i. Organizations have a paramount interest in protecting their resources such as those covered under intellectual property rights, trade secrets, know-how,

competitive strategy, proprietary information, research and developmental strategies. Additionally, other kinds of information or datasets may be acquired by the organizations during the course of their business and for general use by employees during day-to-day activities. These datasets are confidential, and a breach could have significant consequences.

ii. Organizations seek to optimize productivity and increase the output of work, and track employees for this purpose to enhance their commercial gains.

iii. The threats around safety of the workers/workplace could be triggered both by internal and external factors. These could range from, say a machinery deployed at the shop floor or intrusion by a mob. In any case, the organization would be held liable to the extent as found to have failed to discharge its obligations to protect the workspace.

iv. Digital workspaces, particularly where remote working is not only the norm but the preferred mode of collaboration/communication, the boundaries between professional and personal activities have become blurred. In this context, cyber security concerns such as phishing attacks and social engineering are rising rapidly, increasing the likelihood of loss resulting from breach.

The subsequent sections of this document highlight the different concerns and ambiguities surrounding informational privacy of workers and employees at their workplaces. The overarching aim of this document is to provide recommendations to organizations and relevant teams on balancing organizational objectives with ethical and responsible processing of personal data of employees. The first section delves into the various forms that an employer-employee relationship can take, along with the differing degrees of legal obligations involved in each. It also touches upon the definitions of a 'worker' and an 'employee' within the bounds of domestic legislation, exploring which may attract greater labour law and data protection. This is rounded up by an enumeration of five case studies describing scenarios where data protection considerations of an employee may be in conflict with organizational interests, and therefore leading to increased risk of privacy infringements. The second section maps the legal protection afforded to employees' right to privacy across the jurisdictions of the European Union, United Kingdom, China, and the United States, united by the search for policy guidance in this context. The third section approaches each stage of the employment comprising the hiring stage, employment stage, cessation of employment, outsourcing of processing of employment records, and processing data of former employees with the intention to identify gaps in the practices of employers and recommend measures to mitigate the same. The next section deliberates the specific data collection, processing and retention issues plaguing gig workers in the digital economy. On a concluding note, the final section attempts to provide recommendations on best practices for the organizations processing employee data and the different considerations and trade-offs they would need to consider.

2 Context of Employment or Engagement

The terms 'employee,' 'worker,' 'contractor,' 'consultant,' and 'partner' have been used interchangeably taking into account the dynamics of the obligations or liabilities being assumed or distributed between the contracting parties. The traditional definitions of employer-employee relationship vis-a-vis protections guaranteed under the labour laws had been promulgated at a time when the distinction between employment and entrepreneurship was easier to delineate. A brief description of the same is as follows:

Section 2(l) of the Factories Act, 1948:

'Worker' means a person [employed, directly or by or through any agency (including a contractor) with or without the knowledge of the principal employer, whether for remuneration or not], in any manufacturing process, or in cleaning any part of the machinery or premises used for a manufacturing process, or in any other kind of work incidental to, or connected with, the manufacturing process, or the subject of the manufacturing process [but does not include any member of the armed forces of the Union].

Section 2(e) of the Payment of Wages Act, 1936:

'Employee' means any person (other than an apprentice) employed on wages, in any establishment, factory, mine, oilfield, plantation, port, railway company or shop to do any skilled, semi-skilled, or unskilled, manual, supervisory, technical or clerical work, whether the terms of such employment are express or implied [and whether or not such person is employed in a managerial or administrative capacity, but does not include any such person who holds a post under the Central Government or a State Government and is governed by any other Act or by any rules providing for payment of gratuity].

Contemporarily, multiple models of work have evolved in order to support various functions for meeting business objectives. Some of them have been listed below:

i. Deployment of manpower through third parties: This is a model where skilled human resources via third party contractors are deployed on-site by the organizations for various terms of the project. These third parties remain in

control of the terms of service of the workers for the most part. However, the worker is engaged directly by the organization that gets the work done. The typical employer-employee relationship gets moderated through an intermediary, i.e., the third party.

ii. Consultants/Freelancers/Subject Matter Experts: These workers are engaged on various terms relating to duration, deliverables and compensation.

iii. Interns, Apprentice, Volunteers, Assistants: These include personnel engaged for a specific period/project, who may be paid or unpaid, wherein they are expected to gain practical exposure during the term of their engagement with the organization.

iv. Gig workers: The word 'gig' is used to describe a project that lasts for a short period. In the 1900s, it was used by musicians to describe a single performance/act. Now, it is used by cab aggregators, ride hailing applications, delivery applications and similar service providers for 'independent partners' or 'independent executives,' not falling in the traditional definition of employee or subcontractor. In most of these cases such aggregators identify themselves as 'digital intermediaries' and hence may be able to avoid all compliances that arise as a consequence of such engagements. The legal status of individuals working through such platforms has been debated across jurisdictions globally. While in some jurisdictions these workers have been granted recognition as 'employees' of the companies on whose platforms they offer their services, in other jurisdictions courts have ruled in the favour of the service companies by stating that these individuals operate as contractual workers and not as direct employees.

v. Employment Applicants: Seeking employment upon vacancies advertised, or those who submit their resumes voluntarily for future references.

In the above-mentioned kinds of employment or work, there may not be stringent documentation or oversight over the processing of personal data due to the informal, and often short-term nature of relationship between an organization and a worker. This can lead to scenarios where there is a lack of clarity surrounding the purpose for which personal data is collected, involves excessive and unregulated collection of personal data, etc. A lack of governance and accountability here could detrimentally impact the data protection and privacy rights of individuals who engage in this type of informal work.

Moreover, it is difficult to rely on consent as a valid ground for processing in this scenario as the requirements of 'free' and 'unambiguous' consent cannot be fully established between unequal negotiating parties, more so where one of the parties (employee) is dependent on the other for economic benefits.

With the increased adoption and integration of technology into the workplace, it becomes even more critical to delineate guidelines for processing of personal data in the context of employees. Rapid digitization, as well as data-driven decision-making has become so pervasive that it is extremely difficult to escape forms of data processing that happen as a by-product of activities.

The case studies given below are hypothetical scenarios which are inspired from various reports across jurisdictions about the manner in which workers are monitored at their workplaces and the decision-making processes that may impact them based on the data collected.

Case Study 1:

Organization 'ABC Ltd.' is a digital learning and education company where employees work remotely. To track the activity of its employees, ABC Ltd. installed software on the laptops provided by the organization to track screens in real time, record the browsing history, chats, and documents worked upon as they are opened. An 'efficiency' report gets generated on a weekly basis that is reviewed by the managers, enabling them to keep a record of workers' productivity and sanction corresponding salaries. The software is equipped to flag 'suspicious behaviours,' in addition to high-definition cameras that tracked the entirety of daily activities, including breaks taken by the employee.

Case Study 2:

At an IT services company, a tool is deployed to monitor and record keystrokes of employees to measure effectiveness and account for the number of hours spent working on a specific project. Logging of keystrokes is also used to investigate employees who are suspected of accessing proprietary information without authorization. The granular level of tracking prevents the employees from taking any breaks and forces them to work relentlessly for longer shifts.

Case Study 3:

An IoT devices startup files a patent for a connected wearable device for employees to track the location of the workers and nudge them in the direction of their next assignment. The monitoring software which is part of the IoT device's ecosystem is also capable of making automated recommendations to the HR department to fire the workers if they fail to meet the efficiency requirements.

Case Study 4:

A retail brand onboards hundreds of contractual workers to manufacture clothing in their factories operating offshore. To maintain oversight over the workers, factory managers maintain a centralized repository of worker profiles containing records on their family medical history, religious views, and health information. This information was collated by managers during informal chats regarding family issues or religious beliefs, which were then stored and used to evaluate work performance and make employment decisions.

Case Study 5:

At XYZ & Co., a multinational conglomerate, its headquarters recently deployed AI-powered CCTV cameras in the premises which claim to accurately predict the mood of the employees and workers by analyzing facial expressions. Access to certain facilities and rooms in the headquarter premises of XYZ & Co. is restricted only to 'happy' or 'cheerful' employees, an assessment made by the proprietary AI algorithms with the intent to make the workspace a 'lively' place.

The above scenarios provide an insight into the different layers of data protection concerns that arise from rapid adoption of emerging technologies for employee monitoring and evaluation. The next section of this document uses these scenarios as the foundation for examining the relevant regulatory developments in various jurisdictions.

3 Guidance from Global Jurisdictions

This section intends to examine the guidance on privacy of employees from jurisdictions across the world, with special reference to the EU, US, U.K. and China.

European Union

In the European Union (EU), personal data may be processed under any of the lawful bases under the General Data Protection Regulation (GDPR), however, in the context of employment, consent cannot be said to be freely given due to the power imbalance between the employee and the employer. As a result, employers often rely on the performance of contract and pursuance of legitimate interest as the basis for processing an employee's personal data.

Under the framework of the GDPR, EU member states have been encouraged to make specific rules on the processing of employees' personal data, especially for conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, and the implementation of legal obligations.[1] Personal data processed in the employment context lies on a wide spectrum beginning from the recruitment process, performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organization of work. Depending upon national requirements, existing practices and the interest of the workforce, member states may promulgate or amend such laws as may be necessary. These rules should include suitable and specific measures to safeguard the data principal's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings or a group of enterprises engaged in a joint economic activity, and monitoring systems at the workplace.

The Article 29 Data Protection Working Party has also issued an opinion on data processing at the workplace, touching upon data processing during recruitment, in-employment screening, monitoring at home and in the workplace using ICT, use of mobile devices and vehicles, and tracking time and attendance via video

management devices. It serves as a starting point for the member states to address risks to privacy rights of the employees in their respective jurisdictions.[2]

The Data Protection Commission of Ireland has issued comprehensive guidance notes relating to the data protection at workplace and employer obligations,[3] use of CCTVs for data controllers (employers in this case),[4] employer vehicle tracking[5] and processing COVID-19 vaccination data in the context of employment and the work safety protocol.[6]

Datainspektionen, the Swedish Authority for Data Protection has published a guidance for both private and public employers to process personal information collected from employees in accordance with the GDPR thresholds. In addition, they have also released guidelines on the video surveillance of employees.[7]

In France, the country's national data protection regulator, CNIL has also released similar guidance, where the term 'employee' has been defined in a broad context to include permanent employees, temporary workers, interns and trainees, civil servants, and apprentices.

United Kingdom

In the UK, the Information Commissioner's Office (ICO) has published the Employment Practices Code, and started consultation for developing guidance around 'monitoring at work.' Monitoring of workers is to be done in a manner which is lawful and fair to the employees, constantly incorporating established data protection principles in all forms of occasional or systematic technologies or purposes. There are six lawful bases that an employer can choose from while processing employee data (consent, contract, legal obligation, vital interests, public task and legitimate interests), the selection of which must meet the three-part test given by ICO of legitimate purpose, necessity, and balance. The least intrusive means to achieve the selected purpose must be used, especially if the employee is working from home, marked by a higher expectation of privacy. Furthermore, consent as a basis for processing may only be relied on where it is clear, explicit, and workers have control and choice over the monitoring. There is no legal bar on covert monitoring, although organizations are encouraged to follow certain baseline rules regarding the time frame of covert monitoring, the purposes permitting it, and balancing the rights of the employees against them. Workers have the right to object to monitoring and biometric access control mechanisms where the legitimate purpose relied on is (i) public task (for the performance of a task carried out in the public interest or for the exercise of official authority vested in you); or (ii) legitimate interests.[8]

China

China enacted the Personal Information Protection Law (PIPL) in 2021 which provides for the legal basis and obligations for employers while processing personal

data of their employees in a similar phrasing as Article 88 of the EU law. According to Article 13 of the PIPL, a company can process employees' and job candidates' personal information only upon meeting any of the following three conditions: (i) the individual's consent has been obtained; (ii) the collection is necessary for performing an agreement to which the individual is a party or for implementing HR management rules; or (iii) the collection is necessary for performance of statutory obligations. Consent is not required for (ii) and (iii), but it must be obtained specifically for the collection of sensitive personal information.[9]

In the context of public technical equipment such as facial recognition technology, Article 26 of the PIPL stipulates that personal information can only be collected for maintaining public security with proper signage and the information so collected can only be used for that purpose.

In the context of multinational companies, Article 40 of the PIPL provides that all the personal information collected in the PRC must be stored in the PRC, and periodically deleted and anonymized. Furthermore, for cross-border data transfer, employees' consent and an impact assessment ought to be obtained.[10]

United States

In the US, there is no comprehensive federal legislation. Instead, sectoral and state regulations continue to govern the space. Medical privacy, credit check during background verification, locational monitoring, processing of biometrics and such other activities are regulated either under state specific law or by the Federal Trade Commission (FTC). Under the Health Insurance Portability and Accountability Act (HIPAA) privacy rule, healthcare providers are prevented from giving employers access to employees' medical records directly, unless there is a compelling legal basis to do so.[11] On the other end, California's Confidentiality of Medical Information Act (CMIA) specifically requires employers to protect the privacy and security of any medical information they receive.[12] In the context of background checks, the federal Fair Credit Reporting Act (FCRA) restricts consumer-reporting agencies from including medical and financial information in employee background checks without the individual's authorization.[13] California also has the Fair Chance Act, which restricts when and how employers can inquire about and consider a job applicant's criminal history.[14] In Illinois, the Biometric Information Privacy Act (BIPA) requires organizations to obtain consent from employees if it intends to collect or disclose their personal biometric identifiers, and destroy biometric identifiers in a timely manner. Employers have since faced a number of class action lawsuits for improper storage of employee fingerprints and other biometric data.[15]

India

In India, after several years in the making, the Digital Personal Data Protection Act, came to be enacted in 2023. On processing of data in the employment context, it reads:

"Section (7): A Data Fiduciary may process personal data of a Data Principal […]

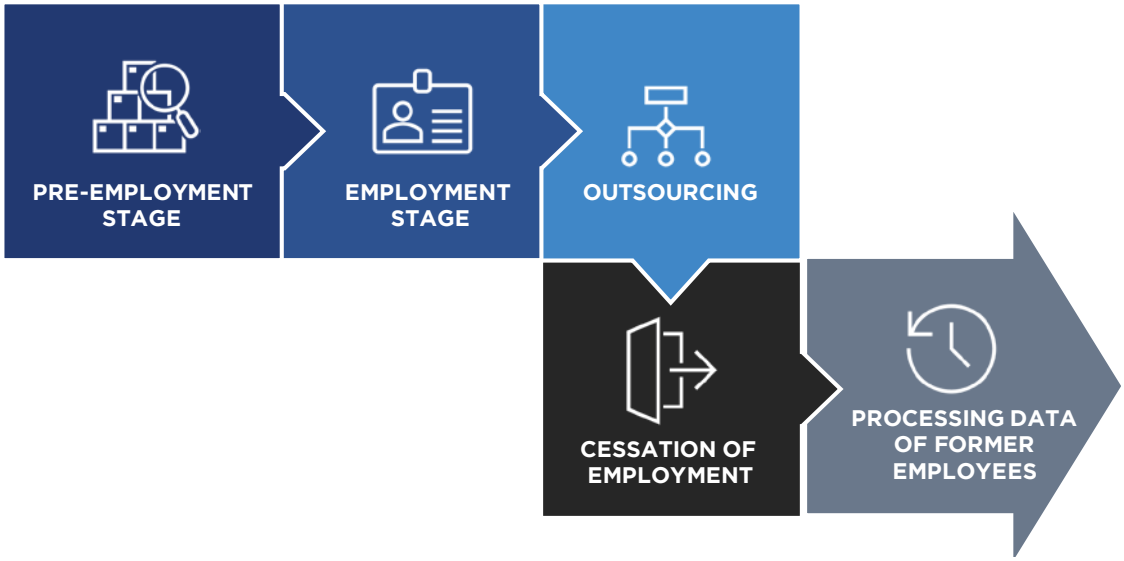
(i) for the purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information for provision of any service or benefit sought by a Data Principal who is an employee. […]"

This section empowers organizations to put in place necessary safeguards to protect and prevent any loss or liability, avoid corporate espionage, and maintain the confidentiality of trade secrets, intellectual property and clients. This also recognizes the collection and processing of the data for any service or benefit that can be extended or sought by the data principal.

The preamble of the Act recognizes that the purpose is to provide for processing of digital personal data in a manner that *recognizes both the right of individuals* to protect their data and *the need to process such data for lawful purposes* and for matters connected therewith or incidental thereto.[16]

Therefore, it is pertinent for organizations to be cognizant of this balance and the need for respecting rights of employees while processing their personal data. Organizations should carefully assess potential negative consequences of data processing activities on their workers and employees, especially when such processing is not intrinsically necessary for their day-to-day operations.

4 Recommendations for Data Processing at Various Stages of Employment



4.1 Pre-Employment Stage

Advertisement

A vacancy or a job opportunity is usually advertised at multiple touchpoints such as the careers or opportunities page of an organization's website, third party job portals, through mailing lists, etc. This stage entails the solicitation of prospective candidates who may be interested in or relevant for the particular role. Sometimes, the details of the organization, contact addresses, and details of recruitment agency are not readily and transparently made available.

Recommendations

i. Such information should be made available conspicuously to enable the applicant to make an informed decision. The soliciting organization must provide a notice to the applicant with respect to the data sought, purposes of processing and the rights exercisable by the applicant with respect to the data collected.

ii. Organizations should strive to minimize the data likely to be collected. Details such as marital status, place of residence, references are not necessarily required at the stage of evaluation for the candidature and therefore this data can be avoided from being collected. Salary slips, previous appointment letters could be required at advanced stages of the recruitment process, but it should be taken only when necessary.

iii. There may be scenarios in which the organization may not prefer identifiability particularly where key hiring or leadership hiring is involved. In such cases, as far as feasible, Personally Identifiable Information (PII) should be redacted, prior to sharing with the organization in order to make the decision for the applicant to be interviewed. The applicant should be notified, and consent be sought for the candidature to be processed. Organizations that acquire the data for such hirings must delete it as soon as the candidature is rejected from being taken forward.

Data collected through job aggregators/intermediaries

Organizations often make use of digital platforms for recruitment. These platforms play the role of aggregators or intermediaries between the job seeker and the hiring organization.

Recommendations

i. The data principals should be appropriately notified about the processing policy of the aggregator, including where the aggregator can be contacted to exercise the right available to data principals.

ii. The data principal must have the ability to delete and/or deactivate their account.

iii. If the data is used for any other purpose such as analytics purpose or as a training data for machine learning, the data principals must be informed and allowed to opt out of such processing.

iv. Intermediaries/job aggregators should devise a policy to deactivate or auto-delete the accounts after a certain period, in the absence of any activity in those accounts by the data principals over a defined period of time.

v. Organizations recruiting through these aggregators/intermediaries must have a valid contract clearly identifying their respective roles and the obligations emanating from each.

Shortlisting of the candidates

A survey published by the Society of Human Resources Management revealed that 79% of employers use tools powered by artificial intelligence, either working towards automating this shortlisting process or having already deployed such tools.[17] The power of AI has the potential to be harnessed in a calculative and risk-based approach to address diversity goals of corporates. The manner in which AI tools have been trained, and the homogeneity and prevalent biases in training datasets used, create great capacity for discrimination on the basis of gender, race, education and age, especially at the stage of selecting candidates. These biases may persist even after direct identifiers have been stripped, as the AI tool may correlate kinds of activities undertaken and education with such categories of community. Such inaccurate tools can certainly lead to discriminatory outcomes arising out of automated decision-making.

In a first of its kind lawsuit filed in 2022 by the U.S. Equal Employment Opportunity Commission (EEOC) involving a company's use of AI to screen out over 200 candidates based on their age, the firm offered to pay $365,000 by way of settlement to the disadvantaged candidates. As on date, the settlement is pending approval of the judge.[18]

This bias may creep in due to various reasons such as faulty or incomplete data set and reflection of social inequalities. While they are often unintentional, their consequences may be severe with a direct bearing on fundamental rights of individuals.

Recommendations

When such technologies are relied upon by employers and hiring agencies, especially in the context of automated decision making, the following aspects must be addressed thoroughly:

i. Notification to the data principal in compliance with regulations to enable them to make informed decisions.

ii. Control on quality and accuracy of data sets used to train the model.

iii. Regular audits to identify risks and eliminate errors which may creep in over a period of time.

iv. Guaranteed right to appeal for independent human intervention and evaluation in order to reassess the output of the model.

v. Governance in terms of explainability, undetected errors, unexplained biases, and security of the lifecycle.

vi. Consistent oversight by human intervention to eliminate or monitor inconsistent results.

vii. Measures to prevent false prompts, hallucination of the model and other black box effects with the potential to materially impact/pollute the processing.

Interview/screening stage

This may be conducted face-to-face with the candidate, or remotely via video/ audio conferencing platforms. Given that virtual meetings are being utilized, particularly at the initial levels of discussion or screening stage, it is important to note that when digital modes are deployed another party comes into the picture, i.e., the digital platform provider. It too processes and records personal data, with or without the knowledge and consent of the candidates and possibly in concomitance with the recruitment agency or hiring firm. Two key considerations here are: (a) ensuring confidentiality of personal data in the case of a virtual/remote interview process, including processing undertaken by the platform provider and (b) the feasibility of providing alternative modes of interview to the prospective candidate. The organizations should, therefore, carefully evaluate the robustness of chosen platforms and their ability to respect and enable privacy considerations.

Additionally, during the interview, personal notes may be taken about the candidate by the panel and/or the digital meetings may be recorded. In either case, the candidate should be informed and advised about the rights that the candidate may exercise in this regard.

On the alternative, during an in-person interview as well, personal data may be collected through various documentation processes, or through recordings captured by the CCTVs installed at the premises of the hiring organization. At this stage, a clear notice should be provided to the candidates informing them of the personal data that is likely to be collected.

Usually, all data forming a part of digital media may be required to be kept for certain purposes, including but not limited to audits, necessitating addressing the lifecycle management of such data through a clear policy.

Recommendations

i. The data principal in these situations should be able to exercise their rights over the personal data stored about them and while the obligation of notification persists, the process by which they can exercise their rights must be clearly delineated.

ii. Interview notes may be kept keeping in view the possibility of any claim of discrimination that may have to be defended, in which case the timeline for destruction of such notes must be laid out at the outset.

Management of recruitment records

Once the candidate is selected and the offer for appointment is accepted by the candidate, the process of recruitment for the said profile stands closed. At this stage the organization will have two sets of data generated, for successful candidates and for unsuccessful candidates.

The records of the unsuccessful candidates may have to be preserved for a certain period in order to establish a defense against discrimination or for any statutory purposes at all. The record of the successful candidate would be moved to the personal file within the organization as soon as the employer-employee relationship commences.

Recommendations

i. Clear identification of the repository (preferably centralized storage) where the data of unsuccessful candidates is stored.

ii. Defined retention period, along with justifiable basis for retention of the data.

iii. Deletion of data from all media, including the backup once the purpose/basis ceases to exist. Where complete deletion is deemed to be too complex or unfeasible, appropriate technologies could be relied upon to anonymize or pseudonymize the data.

iv. Defined process for exercise of the right of data principal during this period.

v. Where the intent is to maintain records for future recruitment purposes, the data principal must be informed of the same as well and allowed to exercise their rights accordingly.

Transfer of data of successful candidate into personal file

Only that data which is required to be carried forward for the purpose of employment should be transferred to the personal file of the employee. Data such as contact numbers or emails IDs taken for reference check must be deleted as soon as the purpose ceases to exist or there is no lawful basis for their retention.

Other material information such as any criminal/civil convictions, penalties, fines, allegations of financial embezzlement, or other such information as may be necessary considering the job role, if collected, should be stored only as long as necessary for a legitimate, justifiable objective. Once the ground ceases to exist, it must be deleted.

Background verification

The human factor is seen as both the weakest and the strongest link in matters relating to security. The employment ecosystem hinges on the pillars of trust and competence. In this case, the person by whom and the manner in which verification is carried out becomes significant. Background verification may be carried out by the organizations to ensure that:

i. The documents, credentials etc. that are represented and submitted by the candidate are true.

ii. Both personal and professional references are correct.

iii. The candidate has not been engaged in any previous conduct detrimental to the current role, for example, examining allegations of financial embezzlement against a candidate may be relevant where the vacancy is for the role of finance director.

ISO 27001 certified organizations are required to conduct background verifications as a part of the compliances required under Information Security Management Standards. While there are no laws which lay down the mode and modality of carrying out background checks, courts have supported the result that in event of suppression or misrepresentation of material facts, the employee can be deemed unfit for employment.*

*In the matter of [*Kiran Thakur vs Resident Commissioner Bihar, 2023:DHC:3459*], the Delhi High Court reiterated that,

"Employees who are guilty of submitting forged documents to their employer, have to be dealt with in a strict manner. If a person submits forged and fabricated documents, then such a person is certainly unfit to be employed. No sympathy or compassion can be shown to such an employee."

Recommendations

In terms of the information obtained, processed, and retained by organizations as part of the background verification process, the following must be kept in mind by them:

i. The candidate should be notified of the same in advance.

ii. Necessary consent must be obtained before the personal data of reference is disclosed.

iii. The data collected for processing and the intended processing must be proportional to the objective pursued.

iv. The third party that is contracted to carry out the due diligence must be evaluated before outsourcing.

v. Supplemental data that gets collected such as phone numbers and email IDs of references, and criminal records if any, must be strictly aligned to the objective, processed only for the limited purpose and deleted as soon as the purpose is over, subject to any other regulatory requirement.

4.2 Employment Stage

During the course of employment, a plethora of personal data is collected, stored, processed, accessed and maintained by the employer. These may fall in the following subheadings:

i. Personal records: Home address, alternate contact details, educational details, previous employment details.

ii. Personal data of family members (spouse, kids, parents): Insurance, health data, financial records.

iii. Financial record: Compensation details, tax information, salary accounts details.

iv. Medical record: Sick leaves, Insurance claims, Accidental/ Injury claims, reimbursements on account of sickness, vaccination certificates.

v. Performance records: Training, skill developments, courses, awards, achievements, appraisals.

vi. Monitoring of data: In the context of Diversity, Inclusivity & Equity (DEI).

vii. Data processed as part of operational requirements of the role. Such processing activities have been enumerated as follows:

    a. Tracking the attendance of the employees: This enables the employer to note working hours for the purposes of payroll, leaves and entitlement purposes. This data is also used for the purpose of optimizing the workforce/workload ratio. Over the years with technology becoming an all-pervasive element, the mode of monitoring working hours has changed from manual to technology-driven. Mobile and screen recording apps have also been developed in order to track real-time geolocations along with the screen time, log-in and log-off times. Along with the requirement of notice in simple, plain and clear language, the employee must be provided an opportunity to opt out of such tracking, especially after officially delineated office hours.

b. Tracking of productivity/efficiency: Such tracking may be undertaken in the guise of security by recording the keystrokes, internet visit, personal work, and review of work emails. With the onset of pandemic, and the acceleration in the remote working models, a certain 'productivity paranoia' has set in. It has been reported that between 2019 to 2023, there was a consistent increase in the global demand for employee monitoring software.[19] From these statistics it is clear that demand for a such software reached an all-time high during the pandemic and then has seen a slight decline, however, it prevails significantly to this day.

   While the use of these technologies in the enhancement of productivity remains an interesting debate, the lack of proportionality between the objective set out to be achieved and the means deployed cast doubt on their privacy aspects. Security needs of an organization may not justify all forms of compromises to privacy and data protection principles. In addition, given the likelihood of false alarms considering that a lot of these technologies are powered by generative AI, the possibility of bias, discrimination and errors cannot be ruled out.

c. Monitoring the systems, internet access, and use of office equipment: Surveillance of the network emerges from the need to constantly detect and defend the network from any internal or external threat that could lead to loss of data. It has been seen that organizations that are fully transparent with their methods and motivations will have higher acceptances while deploying technologies and will be in a position to minimize invasiveness into 'expected' privacy. Monitoring may be of two types, systematic and occasional. While a one-formula-fits-all approach cannot be taken to identify whether the type of monitoring is permitted or prohibited, it may be noted that any 'adverse impact' of monitoring on individuals must be justified by benefits to the employer, other employees and the public. This is where the need for 'impact assessment' arises. This impact assessment would involve stages of defining the purpose, mode of monitoring, identifying risks, mitigation methods and alternative methods of meeting the objective. This further enables evaluating the proportionality of the need of monitoring with the legitimacy of the purpose. Both the monitoring policies and Acceptable Use Policy (AUP) should be made available to the employees during the onboarding process itself. Employees must be adequately informed in advance with reference to the audit trail, registration or log that is created in the course of their activities and that these may be reviewed where violation of workplace guidelines may have taken place.

d. Processing of biometric and facial data: This includes data collected from installation of CCTVs on the floor, biometric processing such as use of facial recognition technologies, voice, iris scanning, fingerprint verification, hand geometry, and gait. These verification methods are used since they are

harder to manipulate or breach, implementation is affordable and provides a mass, long-term solution and the complexity of the process is reduced. In terms of risk assessment, while the probability of compromise is low, in the event of a compromise the damage will be irreversible. Passwords can be replaced, biometrics cannot be. This becomes even more impactful with the integration of technology and high reliance upon some of these tools in healthcare, or auto space, wherein the magnitude of harm could be close to irrecoverable.

CCTV surveillance in high-risk areas can help in identifying potential hazards, aiding in accidental investigations, protecting the space from unauthorized intrusion, and preventing abuse or harassment. However, it must be used with appropriate safeguards and in proportion to the objective required to be met.

When designing a CCTV system, clear requirements, a comprehensive needs analysis, survey of the area to be covered, and appropriate equipment selection and installation must all be considered. The CCTV must also be conspicuously marked at all times. The policy around processing, storage, sharing of data, access, purpose and retention should be readily available for reference.

e. Call recordings in customer-centric roles: The recording of employees' telephonic conversations presupposes that the recording is suitable and necessary for the purpose for which the employer is to record the employee's conversation, e.g., for training purposes, establishing a defense or identifying the grievance. The employee must be made aware of these recordings, the purpose of these recordings, and context of processing. Further these recording must have a defined period of storage and thereafter they must be deleted.

Recommendations

i. The information stored by organizations during the course of employment is likely to be processed on different bases including compliance with a regulatory requirement such as for filing taxes or Provident Fund (PF)/retirement benefits or to establish a defense in event of a claim. There would be other documents that may be processed to facilitate claim such as insurance or medical benefits.

Each of these grounds of processing must mandatorily be aligned with the proportionality of the data so collected and stored vis-à-vis the term for which the said data is retained in the system. Data principals must be informed about this data being stored and processed and should have the right to get it corrected or updated as may be necessary.

ii. When the processing of the data is based on a statutory requirement or required to establish a defense, the right of employee to get the said data erased may be in conflict. In this case an explanation of the same should be accorded along with suitable reasons such that the employee is able to make informed decisions or seek further remedy.

iii. Careful and deliberate evaluation must be undertaken to identify the relevant basis for processing employee data. Consent is usually not an appropriate basis due to unequal bargaining power between employer and employee/worker and because of certain unavoidable organizational interests which require processing of employees' data.

iv. Monitoring every activity of employees may be disproportionate and excessive. Therefore, the employer is under the duty to seek other less invasive means to protect the objective. If it is inevitable, appropriate notice should be provided clarifying the purpose and proportionality. The notification requirement, however, may be eliminated in exceptional cases of covert monitoring. Where authorization may be required for monitoring, the same should be obtained prior to the commencement of the monitoring process.

v. Data collected during the recruitment process should generally be deleted, subject to the requirement of retention under other regulations, as soon as it becomes clear that an offer of employment will not be made or has not been accepted by the individual concerned.

vi. The employee may be advised to update and confirm the accuracy of their records on a regular basis.

vii. The employee should be granted access to their system records only. Wherever appropriate, privacy enhancing technologies must be used to maintain the security of the data.

viii. Sufficient and appropriate controls must be ensured, strictly on a need-to-know basis to those who may have access to this information for the purpose of processing.

ix. The system must be able to create audit trails, capable of demonstrating access and modifications made to the database.

x. With reference to those who have access to this personal information of the other employees, they should execute a non-disclosure agreement that prevents any unauthorized disclosure of this information to a third party. Where this activity is outsourced to a third party, the same should be done under a valid

contract with all appropriate measures, including the right to audit. The liability of the data fiduciary would continue irrespective of its agreement with the data processors.[20] This implies that data fiduciaries must ensure responsibilities/ liabilities irrespective of any other arrangements whatsoever. Contractual interpretation, role definitions and obligations would only be a secondary consideration.

xi. Statutory disclosures under regulations or for investigations is mandatory, and the organization may also include this as a part of their policy of disclosure. Certain data may even be sought by the investigating authorities or other data fiduciaries as authorized by the government.[21] In such cases, the only safeguard that the organization can rely upon, depending upon the context and evolution of regulations, is to verify within available means whether the sharing of this data is obligatory. Where the information is sought with urgency, a decision must be taken carefully taking into account the impact on the individual when it is provided or not.

xii. The 'means' by which the data gets collected and the 'purpose' for which the data gets processed must be communicated transparently to the employee. If there are less intrusive methods to collect the data to meet the same objective, that method should be preferred. The test of selecting the method should be its proportionality as against the intended objective in that context.

xiii. Many organizations such as those which have diversified businesses or are part of the same group tend to have centralized record management systems. These systems are usually the repositories of talent database that are accessed by various divisions based on need. It is pertinent that these databases should be sanitized for clear identification of scope and basis of processing, retention timelines and subsequent deletion of the data set from the system.

4.3 Outsourcing the Processing of Employee Records

Many organizations choose to outsource certain processing activities to third parties. When processing data on behalf of the organization, these are termed as 'Data Processors'. 'Processing on behalf of the data fiduciary' means that the data fiduciary continues to determine the means and purpose of processing and that the processor simply follows the instructions as provided by the data fiduciary. Section 8 of the Digital Personal Data Protection Act 2023 requires that the data fiduciary remain responsible for the acts of the data processor irrespective of the arrangement, over and above a valid contract. Thorough due diligence must also be undertaken with respect to the third party prior to the decision of outsourcing.

Recommendations

i. The obligations and rights should be clearly defined.

ii. The portion of the lifecycle of the data that is entrusted for processing with the processor should be defined.

iii. The technical and organizational measures as required to protect the confidentiality, integrity and availability of the data should be specified.

iv. Reserving a right to audit by the data fiduciary or through an independent third party can further strengthen the oversight over the data processor.

v. Upon completion or cessation of the purpose, the data is appropriately dealt with (deleted, returned, archived).

vi. Where transfer to another jurisdiction is affected, it is pertinent to check specific regulations governing such transfer.

4.4 Cessation of Employment Records & Disclosures

Disclosures and communication required at workplace

Employment may end by virtue of resignation, completion of the contractual term, dismissal or death. In each of these cases or depending upon the circumstances certain disclosures may be necessary. For example, for senior leadership, a cessation could also lead to speculations in the industry. Likewise, dismissal/resignations may lead to questions within the workforce. In such cases the employer may have to share information to maintain trust and transparency at the workplace. This disclosure however would be limited to what is strictly necessary.

While the employee's access to the systems and network is disabled at the time of their exit, the official email account may be kept active for a short-term taking into account factors such as position, role, and presence or absence of a backup. While these decisions should be made after due consideration of the need versus the risk, some safeguards may also be adopted.

Recommendations

i. Auto-reply be inserted with the notification of cessation of the ID and the details of alternate ID for further communication. If feasible, auto forwarding option should be preferred.

ii. This account should be strictly monitored with access to those people only who need to access the account for official purposes.

iii. In the course of employment, it is likely that pictures, photos, thoughts may be uploaded to the website, intranet, and common shared spaces. Employees should be notified such that they would be mindful of the usage of such photographs, and they must be given the option to opt-out of such posts. However, this will have to be balanced against the legitimate objectives of the organization and rights of other employees. To the extent feasible, such references, pictures, data sets may be deleted, subject to any other requirement of the law.

Identification of the records required to be preserved

Employment has legal consequences in terms of rights and obligations defined for the parties under the statute. The employer has various duties to be discharged even after the employer-employee relationship ceases. Therefore, classification of the records is essential to identify the purpose and basis for retaining them. In addition to this, the retention term must be defined according to the basis of retention and the purpose of retention.

4.5 Processing Data of Former Employees and other Workers

In addition to the data processed in the context of employment, there are various other cases of processing of personal data such as interns, former employees, subcontractors, consultants, and manpower supplied through third parties, who do not fall directly within the category of employees.

In all these cases the fundamental balance remains between the rights and freedoms of those engaged vis-à-vis the interest of the organization to defend itself from loss or liability.

Recommendations

i. Collect the bare minimum personal data, sufficient to meet their objective. Anything more is not only a compliance burden but also enhances the risk.

ii. Define the basis and purpose of the processing of the data.

iii. Wherever applicable and feasible assess the legal obligations that may arise and that may devolve a statutory liability to process the data.

iv. Execute valid contracts with third parties who may remain in control as principal employers for the resources deployed to ascertain clear statutory obligations. This further helps in minimizing the need for storage and processing of data of the data principals.

v. Whenever feasible, inform, advise, build consensus with respect to the technology deployed and the objective required to be met.

5 Processing Workers' Data in the Digital Gig Economy

According to NITI Aayog's policy brief, it is estimated that as of 2020-21, 7.7 million workers were engaged in the gig economy.[22] This workforce is expected to expand to 23.5 million workers by 2029-30.[23] The privacy concerns surrounding the processing of personal data of workers on these digital platforms are amplified by the legal ambiguity surrounding their employment status.

For instance, food-delivery platforms in India collect KYC documents, copies of valid government issued vehicle registration certificate, vehicle insurance copy, driving license, identity proof, residence proof, location data, and proof of ownership of the vehicle.[24] Collected data may be utilized for business purposes and needs, background check, verification, marketing, service, development, analytics, research, and other purposes.[25]

As mentioned in the previous sections, freelance services have emerged as a relatively new business model. Information collected by these platforms about the individual performing tasks on their platform includes their email address, name, physical address or billing information, contact details, educational and professional details, and additional authentication information (such as copies of government issued ID, passport, or driving license, as permitted by applicable laws). A huge amount of personal data, besides the name and phone number, such as geolocations, trips undertaken, hours of working, customer ratings along with such other data that is essentially intrinsic to such workers, gets processed, based on which algorithmic decisions are made.

On platforms for freelance services, the entity acts as a marketplace connecting individuals, requesting the performance of tasks in return for some amount of money with individuals across the globe working remotely. In this context, the traditional relationship of an employer-employee does not exist, however, a large amount of personal data is collected on these platforms and processed. Some of the common challenges as highlighted at different forums are as follows:

i. Explainability of deployed algorithms: In many cases it has been reported that such platforms lack transparency in rules for allocating work and evaluation of deliverables. Workers are often evaluated according to processes that have

either not been explained to them or they are not aware of, or it is done in an undisclosed manner. Many of them are unaware of the consequences until they actually happen.

ii. Suspension from the platform or closure of accounts: Multiple complaints and concerns have been made against suspension of freelance workers' accounts due to failure of identification system or sometimes, simply undisclosed reasons. In certain cases, fees were stalled by the platform aggregators and the worker was left with no recourse.

Recommendations

i. The requirement of notification and limitation of processing must be followed from the point of collection of personal data to its lifecycle management including but not limited to its usage for defined purpose.

ii. Systems, algorithms, and logic deployed for processing of the data must be explainable, transparent, fair and accurate. When a decision capable of having an impact on the rights and freedom of a person is to be taken, the right to appeal to a human evaluator is strongly recommended.

iii. The right to contest such decisions must be availed and having a third party evaluator would further strengthen the commitment to anti-discrimination.

6 Conclusion and General Recommendations

The global COVID-19 pandemic fundamentally changed the manner in which the workspace was defined. With work from home becoming the preferred option, organizations, employees and workers witnessed a fundamental shift in their experience of work and productivity.

In an interesting case presented before the Irish DPA, an employee, while working from home, printed CVs and ended up placing them in domestic recycling bins, and the paper documents were dispersed with a blow of the wind. The DPA observed that, *"while it is important for staff to understand and implement good data protection practices, it is the responsibility of the controller to ensure that they do so and have the means – including, where appropriate, devices such as shredders - of delivering the required standard of protection."*[26]

This case becomes particularly interesting because changes in the work environment can impact the various measures in place and adopted by the organizations. With the growing recognition of remote working scenarios, it is important for organizations to reassess, review and adapt their resources, policies and procedures to ensure that they are adequate for the risks posed and the environment in which they occur.

In this light, and in addition to the specific recommendations laid out in the previous sections of this document, mentioned below are some general recommendations that organizations should be mindful of when processing personal data of employees and/or workers engaged with them:

i. Destruction of records is not only done by clicking on the delete button. It may independently need a process of review and destruction. This may also involve sanitation/destruction of media in which the data was stored, as well as of its backup or adoption of such measures to ensure that data does not continue to be processed.

ii. The use of analytical techniques such as data mining, predictive analytics and contextual analytics to enable managers to take better decisions related to

their workforce could have a detrimental impact on the employees, including discriminatory outcomes. Therefore, their use must be limited to certain purposes which do not have a direct impact on individuals.

iii. Wearables such as smart watches and smart gloves may bring additional value to work by contributing to creating a healthy and safe workplace. However, the data collected by them, if breached, can cause irreparable harm to the data principals. This is the reason why it is widely proposed that data minimization remains the most effective safeguard.

7 References

[1] GDPR Article 4(12), https://www.privacy-regulation.eu/en/article-88-processing-in-the-context-of-employment-GDPR.htm

[2] Article 29 Working Party, "Opinion 2/2017 on data processing at work," https://www.dataguidance.com/sites/default/files/wp29_opinion-dataprocessingatwork.pdf

[3] Data Protection Commission, Data protection in the Workplace: Employer Guidance April 2023, https://www.mondaq.com/ireland/privacy-protection/1344238/data-protection-in-the-workplace--dpc-guidance

[4] Data Protection Commission, Guidance on the Use of CCTV – For Data Controllers, https://www.dataprotection.ie/sites/default/files/uploads/2019-05/CCTV%20guidance%20data%20controller.pdf

[5] Data Protection Commission, Guidance Note: Employer Vehicle Tracking, https://www.dataprotection.ie/sites/default/files/uploads/2020-09/Employer%20Vehicle%20Tracking_May2020.pdf

[6] Data Protection Commission, Processing COVID-19 Vaccination Data in the context of Employment and the Work Safely Protocol, https://www.dataprotection.ie/sites/default/files/uploads/2021-11/Processing%20COVID-19%20Vaccination%20Data%20in%20the%20context%20of%20Employment%20and%20the%20Work%20Safely%20Protocol.pdf

[7] Swedish Authority for Privacy Protection, Video-surveillance of employees, https://www.imy.se/en/organizations/camera-surveillance/videosurveillance-of-employees/

[8] Information Commissioner's Office, Data protection and monitoring workers, https://ico.org.uk/for-organizations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/#dp1

[9] Personal Information Protection Law, https://personalinformationprotectionlaw.com/

[10] Roberto Gilardino, "The Dos And Don'ts Of Processing Employee Data Under Personal Information Protection Law In China," https://www.mondaq.com/china/employee-rights-labour-relations/1201456/the-dos-and-donts-of-processing-employee-data-under-personal-information-protection-law-in-china

[11] HIPAA for Individuals, https://www.hhs.gov/hipaa/for-individuals/employers-health-information-workplace/index.html

[12] California Civil Code, §§ 56.20-56.245, http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=1.&chapter=3.&part=2.6.&lawCode=CIV

[13] Fair and Accurate Credit Transactions Act of 2003, https://www.ftc.gov/legal-library/browse/statutes/fair-accurate-credit-transactions-act-2003

[14] Fair Chance Act, 2018, https://calcivilrights.ca.gov/fair-chance-act/

[15] Federal Trade Commission, FTC Warns About Misuses of Biometric Information and Harm to Consumers, https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers

[16] Digital Personal Data Protection Act 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[17] Gary D Friedman, "Artificial intelligence is increasingly being used to make workplace decisions–but human intelligence remains vital", https://fortune.com/2023/03/13/artificial-intelligence-make-workplace-decisions-human-intelligence-remains-vital-careers-tech-gary-friedman/

[18] US Equal Employment Opportunity Commission, "Press Release: iTutorGroup to Pay $365,000 to Settle EEOC Discriminatory Hiring Suit," https://www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit

[19] TOP10VPN, "Employee Monitoring Software Demand up 60% since 2019," https://www.top10vpn.com/research/covid-employee-surveillance/

[20] Digital Personal Data Protection Act 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[21] Digital Personal Data Protection Act 2023, Section 11(3), https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[22] NITI Aayog, "Policy Brief: India's Booming Gig and Platform Economy," https://www.niti.gov.in/sites/default/files/2022-06/Policy_Brief_India's_Booming_Gig_and_Platform_Economy_27062022.pdf

[23] ibid.

[24] Zomato, "Delivery Partner Terms and Conditions," https://www.zomato.com/deliver-food/privacy-policy

[25] Swiggy, "Privacy Policy," https://www.swiggy.com/privacy-policy

[26] Data Protection Commission, Case Studies 2018-2023, https://www.dataprotection.ie/sites/default/files/uploads/2023-09/DPC_CS_2023_EN_Final.pdf

Author

Abha Tiwari
Data Protection Officer, Vistara - TATA SIA Airlines
https://www.linkedin.com/in/abha-tiwari-708303a/

Contributor

Shivangi Malhotra
Associate- Privacy and Policy, DSCI
https://www.linkedin.com/in/shivangi-m/


DSCI
PRIVACY
LEADERSHIP FORUM