PRIVACY IN THE WORKPLACE

produced by the Office of the Privacy Commissioner for Bermuda (PrivCom)

August 2024

Contents

Introduction

The Office of the Privacy Commissioner for Bermuda (PrivCom) has published a Guide to PIPA for organisations to understand the Personal Information Protection Act 2016 (PIPA).

This guidance document is specifically aimed at assisting employers as organisations regarding their information processing responsibilities, obligations, and duties when using the personal information of their employees, former employees, and prospective employees.

Employers use significant amounts of personal information on prospective and current employees. In some instances, employers may also continue to use the personal information of former employees. This personal information can range from basic information such as names, addresses, and employee numbers, but can also include information on occupational health, sick leave, performance reviews, or disciplinary actions. Therefore, employers ("organisations") must be mindful of their responsibilities, obligations, and duties under PIPA. This includes ensuring they have appropriate policies and procedures in place, as well as understanding how to respond to requests from employees (including former employees and unsuccessful candidates in the recruitment process whose information they may continue to retain) regarding the exercise of their rights under PIPA.

Remember! An individual does not lose their privacy and data protection rights just because they are an employee.

For example, as described in our Guide to PIPA, PIPA requires organisations to designate a Privacy Officer (PO). This also applies to employers in their capacity as organisations.

Is it personal information?

Within the employment context, it is important to distinguish between business contact information and personal information. PIPA applies to personal information, which is a defined term. PIPA does not apply to the use of business contact information for the purpose of contacting an individual in their capacity as an employee or official of an organisation. This type of information is excluded from PIPA's scope under Part 1, subsection 4(c). In many cases, it will be obvious what business contact information or personal information is; however, in other instances, it may be less clear.

Case Study: Employee emails

While it is clear that an individual's name is their personal information, within the employment setting does the content of an email signed off by an individual in their professional or work capacity constitute their personal information? Probably not – because it is business contact information.

As a practical matter, this question is most relevant is if a rights request is made, such as if an individual wanted access to the personal information used by the organisation. Under those circumstances, there is an obligation on employers to investigate the content of their commercial or business emails to ascertain if the content of the email, which may be signed off by an employee, can be considered the personal information of the employee.

> ***Name in a work email address***
> To give an example, work email addresses can be found in different formats, and may or may not include an individual's name. Even if the email address is considered to be business contact information (and therefore not covered by PIPA), the content of the emails addressed to the identified individual may constitute the individual's personal information. PIPA may apply even if the emails occurred within the context of a professional working environment.

When an employer receives an access request, there is an obligation on employers to investigate the content of their commercial or business emails to ascertain if the content of the email relates to the personal information of an individual in any way. In circumstances where an employee has a long employment history with an employer, it may be the case that several thousand emails have been generated during the employee's employment. In cases such as these, PrivCom would advise the employer to ask the employee to specify in their request a particular date or time. The Guide to PIPA for organisations in relation to access requests is available here.

Outlook calendar and job description

As to whether a job description is personal information is best illustrated by the following example:

Scenario 1: An employee's incomplete access request submitted to their employer

In this **hypothetical** example, an employee makes a complaint to PrivCom as they are dissatisfied that they have not been provided with a copy of their personnel file or a copy of their job description when they made an access request to their employer. The employer advised they previously provided the employee (applicant) with a copy of their personnel file and said that a copy of their job description would not be provided as it did not contain their personal information that could identify the individual. In this hypothetical case, PrivCom **would advise** that the job description does not fall under the remit of personal information as defined in Part 1, section 2 of PIPA.

Employer's obligations and responsibilities

(a) General principles and rules

Employers in their capacity as organisations should be aware of the principles of data protection and privacy under Part 2 of PIPA. PIPA establishes principles that require organisations to use personal information in lawful and fair manner (section 8) and meet requirements responsibility and compliance (section 5), conditions for using personal information (section 6), including sensitive personal information (section 7), privacy notices (section 9), purpose limitation (section 10), proportionality (section 11), integrity of personal information (section 12), and security safeguards (section 13). PIPA also provides rules about breaches of security (section 14), transfer of personal information to an overseas third party (section 15), and personal information about children in the information society (section 16).

Employers must be able to demonstrate compliance with all these principles and rules.

To give an example, an employer can demonstrate the presence of transparent processes in the workplace by way of an easily accessible HR self-service system allowing employees to see what information an employer holds on them and how it is used. This system would be documented in internal HR policies and include details of what personal information is collected and used, and what the purpose of using the personal information is. This system could include an employee's address, current employment status, their marital status (married or single), and their salary information. The system would also include an employee's performance review and any sick leave they have taken. Allowing an employee full access to this information demonstrates that an employer is being fair about what information the organisation holds on an employee.

Fairness

Employers in their capacity as organisations must use the personal information they hold on employees in a lawful and fair manner (section 8). Use of personal information must always be fair and lawful. If any aspect of their use of personal information is unfair, employers will be in breach of this principle – even if they can show that they have a lawful basis for the use.

In general, fairness means that employers should only handle personal information in ways that they would reasonably expect, and not use it in ways that have unjustified adverse effects on them. Employers need to stop and think not just about how they can use personal information, but also about whether they should.

Whether an employer's actions are fair depends partly on how they obtain personal information and whether they are being transparent about how they use it. In particular, if anyone is deceived or misled when the personal information is obtained, this is unlikely to be fair.

Privacy notices

Employers must provide individuals such as employees with clear, concise, easy-to-understand information about the purpose(s) for which they process their personal information and the legal condition that they rely upon (privacy notice under section 9). It should be clear to employees when and why their personal information is collected, used, or otherwise processed. Using clear and concise language, this transparent information on uses of personal information should be easy to access and understand for employees.

Specifically, under subsection 9(1) PIPA states that a privacy notice must include:

a) the fact that personal information is being used;
b) the purpose for which personal information is or might be used;
c) the identity and types of individuals or organisations to whom personal information might be disclosed;
d) the identity and location of the organisation, including information on how to contact it about its handling of personal information;
e) the contact details of the privacy officer;
f) the choices and means the organisation provides to an individual for limiting the use of, and for accessing, correcting, blocking, erasing and destroying, his personal information.

Purpose limitation

The purpose for using personal information should be explicit, clear, and determined from the outset – in other words, before or at the time of collecting it. Personal information should only be collected or used for the purposes specified in the privacy notice and for purposes that are related to those specific purposes (subsection 10 (1)). Organisations must record their purposes as part of their obligations to adopt "suitable measures and policies" and specify them in their privacy policy (section 5) and privacy notice (section 9).

For example, if an employer collects personal information, such as the private email address of an employee, for the sole purpose of communicating certain HR matters to the employee prior to commencing employment, the employer cannot subsequently use that private email address of for another purpose or share that email with another organisation in the absence of a legal condition such as consent. This is because the subsequent use is unlikely to be compatible with the original purpose for which the information, i.e., the email address, was originally collected.

Scenario 2: The use of car park and building access data had been used by a manager to verify employee's time and attendance record.

In this **hypothetical** example, a complaint is made to PrivCom in relation to the use of car park and building access data that was used by a manager to verify an employee's time and attendance record. The employer stated the company car park and building access information was collected

for security purposes and for the purposes of verifying time. The employer also stated that attendance in the building was a security concern.

PrivCom would advise that such use of personal information would be deemed further use, incompatible with the original purpose of collecting and using the employee's personal information, as the employer did not inform the employees that such information would be used to verify their time and attendance. PrivCom would recommend that the employer consider an alternative way to verify time and attendance or limit its use of this personal information to the future, after the employees have been made aware of the purpose.

In rare situations, an employer in their capacity as an organisation may be exempt from the full scope of PIPA. However, even in such cases the "minimum requirements" still apply – in other words, organisations must still meet requirements under sections 5 (Responsibility and compliance), 8 (Fairness), 11 (Proportionality), 12 (Integrity of personal information), and 13 (Security safeguards).

The employer must still document how they concluded that a PIPA exemption applies and how their compliance with PIPA would interfere with the exempted purpose. HR-related purposes for using personal information are unlikely to be exempted.

Proportionality

Section 11 requires employers in their capacity as organisations to assess the necessity of their use of personal information. Use of personal information must be **adequate**, **relevant**, and **not excessive** in relation to the purposes for which it is used. Employers must not hold more information than they need for their purposes. Any use beyond what is necessary for the purposes may violate the principle of proportionality.

Note: Other jurisdictions, such as the UK or EU, refer to this principle as "data minimisation".

Integrity of personal information

Under section 12, employers in their capacity as organisations must ensure that personal information used is accurate and kept up to date to the extent necessary for the purposes of its use. Employers must ensure that personal information for any use is not kept for longer than necessary for that use.

Security safeguards

Under section 13, employers in their capacity as organisations must implement appropriate safeguards against the following types of risk that the personal information they hold may be exposed to;

- loss;
- unauthorised access, destruction, use, modification or disclosure; or
- any other misuse.

Employers must ensure that the safeguards are proportional to the likelihood and severity of the harm threatened by the loss, access, or misuse of the personal information.

PIPA does not specify what such appropriate safeguards for protecting the personal information an organisation holds are, so organisations should refer to information security best practices. As an example, encryption is highly recommended.

Breach of security

Under section 14, employers in their capacity as organisations have a duty to report breaches of security to the Privacy Commissioner without undue delay. A personal information breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just losing personal information.

Employers must also inform the employees or any other individuals affected by the breach without undue delay.

Employers should ensure they have robust breach detection, investigation, and internal reporting procedures in place. Employers must also keep a record of any personal information breaches, regardless of whether they are required to notify.

Transfer of personal information to an overseas third party

PIPA applies to organisations in Bermuda. Individuals risk losing the protection of Bermuda's data protection laws if their personal information is transferred outside of Bermuda. On that basis, PIPA contains rules about transfers of personal information to overseas third parties located outside of Bermuda. Individuals' rights regarding their personal information must be protected; or one of a limited number of exceptions must apply.

(b) Legal conditions for using personal information

Under PIPA's section 8, employers in their capacity as organisations must use personal information in a lawful manner. Under subsection 6(1), an organisation may use an individual's personal information in a lawful manner only if one or more of the conditions are met. PIPA section 6(1)(g) states that information may be used if "the use of the personal information is necessary in the context of an individual's present, past, or potential employment relationship with the organisation."

In other circumstances, another condition may apply. We discuss the possible conditions below, and you can see our Guide to PIPA for more information on section 6.

PIPA also considers "sensitive personal information" to be of a higher risk and needing special consideration for safeguards. According to section 7, sensitive personal information includes any personal information relating to an individual's place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information. According to PIPA, employers in their capacity as organisations in Bermuda are prohibited from using sensitive personal information without lawful authority if it would discriminate contrary to Part II of the Human Rights Act. According to PIPA section 7(3)(d), use of such information is only permitted in the context of recruitment or employment where the nature of the role justifies such use. Employers who use sensitive personal information should document how the use is justified.

Employers must determine, prior to using the personal information of their employees, which condition they rely upon to ensure they use the employee's personal information in a lawful and fair manner. Employers may rely on different conditions for using personal information as it relates to their specific circumstances. It is a matter for the employer to make those determinations as to what personal information is required to be processed for what purpose.

The necessity requirement

Most conditions in PIPA's section 6 require that the use of the personal information is "necessary" for the purpose.

Employers should assess what personal information is necessary for the relevant condition and purpose that they rely upon in their use of the personal information.

In assessing necessity, employers should consider the reasonableness and proportionality of the use, e.g.:

- Is there a more reasonable or less intrusive way to achieve the stated purpose without using personal information?
- Can their objectives be achieved by using less personal information?

If so, this alternative ought to be done instead. Otherwise, there is a risk that the condition upon which the employer relies will be unlawful. This necessity element will be a case-by-case assessment, depending on the circumstances of the use of personal information.

Consent

Consent is the most familiar condition for both individuals and organisations. It is a condition for the use of personal information under PIPA's subsection 6(1)(a).

The standard for consent set by PIPA means that organisations may use an individual's personal information only if the personal information is used with the consent of the individual where the organisation can reasonably demonstrate that the individual has knowingly consented.
Employers in their capacity as organisations are obliged to provide clear, prominent, easily understandable, accessible mechanisms for employees to give consent in relation to the use of their personal information.

Employers in their capacity as organisations should make an effort to present individuals with information and choice to ensure the individual understands what they are consenting to.

Employers and public authorities need to take extra care to show that consent is freely given. They should avoid over-reliance on consent.

However, consent may not be an appropriate condition for employers to rely upon for the use of their employees' personal information. Arguably, there is an imbalance of power between employees and employers. The imbalance undermines the level of choice an employee will feel they may have in giving consent.

Where an employer attempts to rely on consent to use employee personal information, the employee must be given an option to withdraw their consent at any time. Employers need to ensure they can facilitate this withdrawal of consent and make that process easy for employees.

Contract

The condition of contractual necessity is a common lawful basis for employers to rely upon, given that a contractual relationship often exists between an employer and employee. Employers should note that the use of personal information should be "necessary for the performance" of the employment contract, otherwise they may need to consider reliance on another condition.

Employers should note this condition only applies where the contract is between the employer and employee. A contract between the employer and a third party cannot fall under contractual necessity as a condition for the use of employee personal information.

An example of lawful basis in this context is the performance of a contract: an employer will need to use an employee's personal information to perform their obligations under a contract, such as processing the employee's bank details to pay the employee.

In assessing if the use of personal information is necessary for the performance of a contract with the employee, employers should again consider if the use is objectively necessary and proportionate, such as:

- Are other alternative and less intrusive measures available?

The contractual terms may themselves specify that certain activities relating to the use of personal information are necessary for the contract. However, all such activities need not be specified within the contract itself, and some of these activities may be covered by the general context of the contract. That being said, an employer will still be required to meet their obligations as set out under PIPA's section 9 (Privacy notices) when relying on contractual necessity as a condition. If the use of sensitive personal information is necessary for the performance of an employment contract, the employer should identify a separate exception to the general prohibition on the use of sensitive personal information under section 7.

Legal obligation

Where an employer in Bermuda is obliged to comply with national law, 'compliance with a legal obligation' may be an appropriate condition to rely upon. However, the requirement to assess necessity of using personal information still applies. Bermuda's laws or regulations do not have to specify the use, but if the overall purpose of the use of personal information is compliance with the law and the law has a sufficiently clear basis, this condition may apply.

The condition must be laid down law applicable to Bermuda, including national law, regulations, or common law.

However, the law must be clear and precise, ensuring its application to an individual is foreseeable. There should be a public interest achieved by the law and it should be proportionate to that aim or goal. A single law may provide a condition for several uses.

An employer should inform their employees of what laws they rely upon or comply with when using employee personal information. Furthermore, an employer will also need to assess the necessity and proportionality of the use to comply with a legal obligation.

An example of this condition used in an employment contract is where an employer will provide employee information to the Office of the Tax Commissioner to comply with tax requirements or to comply with an employer's obligations under the Occupational Safety and Health Act 1982.

Emergency threatening the life, health, or security of an individual or the public

This is not a commonly used condition and will only apply in certain limited specific situations and where another condition is not appropriate.

It generally applies where "the use of the personal information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public" under PIPA's subsection 6(1)(f). So, situations involving threats to the life, health, or security of the individual or the public may give rise to this condition. This condition is most likely to arise in the context of medical information, including a person's mental health. It is less likely to provide a condition outside of emergency situations, though.

A task carried out in the public interest

Most commonly, this condition will be relied upon by public authorities or persons governed by public law, but it can also include professional associations or organisations governed by private law.

Reasonable Person Test

PIPA permits organisations to use personal information if it would not be reasonably foreseeable that an individual would ask the organisation not to use the information.

Under PIPA section 6(1)(b), the organisation may determine that the individual would not reasonably be expected to request that the use of his personal information should not begin or should cease. In such cases, the use of information would probably have only a minor effect. The use cannot affect the individual's interests, rights, or freedoms.

To rely on this condition, the organisation must also determine that the use of personal information does not prejudice the rights of the individual. In addition, the organisation cannot rely on this section if the use relates to sensitive personal information.

Employers will still need to consider the necessity of the use of personal information, the proportionality and if any less intrusive measures are available. Overall, employers need to consider if the use is reasonable, which will depend on the circumstances of the case.

An example of this type of processing would include the use of CCTV for the purpose of monitoring building security. A risk assessment in this instance should take note of the legitimate interest of the employer to ensure the security of their building whilst also noting the rights and freedoms of their employees. The employer should ensure that the CCTV is used for the specified given purpose only and not to monitor employee entry and exit times, unless specified in any internal policy.

Sensitive personal information

Section 7 of PIPA defines special category personal information as:

"[...] any personal information relating to an individual's place of origin, race, colour, national and ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, and biometric information or genetic information."

There is a general prohibition of using sensitive personal information subsection 7(2):

"No organisation shall, without lawful authority, use sensitive personal information identified in subsection (1) in order to discriminate against any person contrary to any provision of Part II of the Human Rights Act 1981."

However, there are exceptions to this prohibition contained under subsection 7(3):

"For the purposes of subsection (2), sensitive personal information is used with lawful authority if and only to the extent that it is used—

(a) with the consent of any individual to whom the information relates;

(b) in accordance with an order made by either the court or the Commissioner;

(c) for the purpose of any criminal or civil proceedings; or

(d) in the context of recruitment or employment where the nature of the role justifies such use."

(c) Occupational health

Occupational health refers to the promotion and maintenance of the health, safety, and welfare at work of [every employer's] employees. In Bermuda, occupational health is underpinned by the Occupational Safety and Health Act 1982 ("the 1982 Act"). Section 3 of the 1982 Act outlines the general duties of employers when ensuring the safety and health of their employees. The 1982 Act places obligations on both employers and employees to ensure that the worker is fit to carry out their duties in the workplace. Under subsection 9(h) of the 1982 Act, "the Minister may make regulations requiring the making of arrangements to promote the health of persons at work, including arrangement for medication examinations and health surveys".

The referral of an employee to undergo a medical examination by a registered medical practitioner, within the meaning of section 2 of the Bermuda Health Council Act 2004, may give rise to data protection and privacy implications under PIPA, in particular section 7 (sensitive personal information). As previously outlined, employers must determine, prior to the use of personal information, which condition they rely upon to ensure that they use employee personal information in a lawful manner. It is best practice for employers to outline this condition to their employees in a privacy notice in order to ensure compliance with the privacy principles set out in PIPA.

In an occupational health context, certain lawful bases for processing may apply, such as subsections 6(1)(d), 6(1)(f), and 6(1)(g) of PIPA. Consent may also apply as a lawful basis for using an employee's medical information, although limitations may apply. Under PIPA's subsection 6(1)(a), an employer may use an employee's personal information only if the personal information is used with the employee's consent where the employer can reasonably demonstrate that the employee has knowingly consented prior to the medical examination.

An employer's obligations under sections 5, 8, 10, and 11 of PIPA includes the implementation of appropriate measures and policies which ensure the use of personal information in a lawful and fair manner. The inclusion of an occupational health policy will allow both the employer and employee to engage with registered medical practitioners to the extent necessary to ensure the employee's fitness to work is guaranteed.

Section 18: Access to medical records

Under PIPA, individuals have the right to access their medical records. Medical records or other health-related information is sensitive personal information.

Subsection 18(1) says:

1. On the request of an employee to access
   (a) personal information of a medical or psychiatric nature relating to the individual; or
   (b) personal information kept for the purposes of, or obtained in the course of, the carrying out of social work in relation to the individual,

an organisation may refuse to provide access to personal information if disclosure of the personal information to the employee would be likely to prejudice the physical or mental health of the individual.

If the employer refuses to grant a request by relying on subsection 17(2) or pursuant to section 17(3), if requested to do so by the employee, they are obliged to provide access to the personal information to a health professional, who has expertise in relation to the subject matter of the record, and the health professional shall determine whether disclosure of the personal information to the employee would be likely to prejudice their physical or mental health.

If an employer is reasonably able to redact information which is referred to in subsection 17(2)(b) or subsection 17(3)(b) or (c) from other personal information about them, the employer is obliged to provide the employee with access to the other personal information after redacting the former information or the information which would be likely to prejudice the employee's physical or mental health.

(d) Employer policies and employee monitoring

Introduction

Subsection 5(1) requires employers in their capacity as organisations to "adopt suitable policies and measures to give effect to [their] obligations and to the rights of [employees]", including for compliance with section 13 (security safeguards) of PIPA. Although PIPA does not specify the policies, measures, and safeguards, they include technical and organisational measures within the employment context, such as, but not limited to, pseudonymisation, anonymisation, limiting access to personal information to authorised people, encryption, backups, testing, and maintaining file access audit logs.

Employers may wish to implement data protection policies specifically for the processing of employee information and a separate policy for the processing of any personal information of clients or members of the public. Employers may also wish to have separate data retention and storage, internet usage, use of personal device and CCTV policies for employees and clients or members of the public. Those policies will need to meet the obligations set out under section 9 (privacy notices) and must be "a clear and easily accessible statement [...] about [their] practices and policies with respect to personal information".

In addition to employer policies, employers are required to consider their relationship with any third parties who process information on their behalf in connection with them. In this regard, appropriate agreements need to be in place between employers and third parties.

CCTV and vehicle tracking

For information on CCTV privacy risks and best practices, please see our guidance note.

Because of the potential risk of harm in real-time location tracking, in order for in-vehicle tracking to be lawful under PIPA, strict requirements must be met by the employer. Vehicle tracking should not be used for the general monitoring of staff.

Computer networks, internet, and email

PrivCom accepts that employers in their capacity as organisations have a legitimate interest in protecting their business, reputation, resources, and equipment. To achieve this, employers may decide to monitor their staff's use of the internet, email, and telephone. However, it should be noted that the collection, use or storage of information about workers, the monitoring of their internet access or email, or their surveillance by video cameras (which process images) involves the use of personal information and, as such, PIPA applies.

Under the European Convention on Human Rights, Article 8, individuals have a right to private life, including at work. In addition, the European Court of Human Rights (ECoHR) judgement in the

matter Barbulescu v. Romania (application no. 61496/08) highlights the necessity for appropriate care in monitoring employees and setting clear policies. Therefore, such practices and policies should reflect an appropriate balance between the legitimate interests of the employer, and the data protection and privacy rights of the employees.

As an illustrative example, the European Data Protection Board (EDPB)'s Guidelines 3/2019 on processing of personal information through video devices acknowledges that while some individuals may be comfortable with the use of video surveillance for security purposes, 'guarantees must be taken to avoid any misuse for totally different and – to the individual – unexpected purposes (e.g., employee performance monitoring)'. Furthermore, it states that 'an employee in his/her workplace is in most cases not likely expecting to be monitored by his or her employer.'

An individual does not lose their privacy and data protection rights just because they are an employee. Any limitation of the employee's privacy rights should be proportionate to the likely damage to the employer's legitimate interests. An acceptable usage policy (AUP) should be adopted, reflecting this balance, and employees should be notified of the nature, extent and purposes of the monitoring specified in the policy. In the absence of a clear policy, employees may be assumed to have a reasonable expectation of privacy in the workplace.

The following points need to be addressed by organisations/employers in their policies, notices, and other communications to employees:

- The needs of the employer to use personal information that is necessary for the normal development of the employment relationship and the business operation.
- Monitoring, including of employees' email or internet usage, surveillance by camera, video cameras, or location data must comply with the requirements of PIPA. Staff must be informed of the presence of surveillance in the workplace and of the purpose for which personal information is to be used. If CCTV cameras are in operation, and public access is allowed, a notice to that effect should be displayed. Any monitoring must be carried out in the least intrusive way possible. Only in exceptional circumstances associated with a criminal investigation, and in consultation with the Police, should employers resort to covert surveillance
- Monitoring and surveillance, whether of email use, internet use, or in terms of video cameras or location data, are subject to data protection and privacy requirements and obligations under PIPA. Any monitoring must be a proportionate response by an employer to the risk they face, considering the employees' privacy and other interests.
- Staff should be made aware of what information an employer is collecting on them in line with the principles in section 9 of PIPA. Staff have a right to access a copy of their personal information under section 17.

- Any personal information used in the course of monitoring must be adequate, relevant, not excessive, and not retained for longer than necessary for the purpose for which the monitoring is justified.
- Appropriate safeguards ought to be in place, particularly if the monitoring is intrusive. In Barbulescu v. Romania, the ECoHR held that such safeguards ought to ensure "that the employer cannot access the actual content of the communications concerned unless the employee has been notified in advance of that eventuality".

Internet

Private use of the internet in the workplace and the monitoring of private emails pose certain challenges. A workplace policy should be in place in an open and transparent manner which should ensure that:

- an impartial balance is struck between the legitimate needs of employers and the personal privacy rights of employees;
- any monitoring activity is transparent for all workers;
- monitoring is fair and proportionate with prevention being more important than detection.

Employers should consider whether they would obtain the same results with less intrusive measures of supervision.

Employee monitoring software

Monitoring software and applications are highly intrusive and any attempt to use it must be objectively and demonstrably justified and proportionate. In the duration of an individual's employment, employers should implement other, less intrusive means, by which they can monitor employees' attendance and productivity.

If an employer wants to install covert software, by way of keystroke logging, "bossware" or "tattleware" or other monitoring software programmes on an employee's PC or laptop to investigate possible misconduct, or to monitor an employee's activity when working in the office or working remotely, the use of recording mechanisms to obtain information without an individual's knowledge is generally unlawful.

All employees should be given an Acceptable Usage Policy (AUP), i.e., a policy on email and internet use in the workplace, setting out in clear and easily accessible terms an employer's policy on internet usage, including the use of social media on an employer owned PC or laptop.

Covert surveillance in the workplace

Covert surveillance should be avoided where at all possible. It is normally only permitted on a case-by-case basis where the information is kept for the purposes of preventing, detecting, or investigating offences, or apprehending or prosecuting offenders. A written, specific policy should be put in place detailing the purpose, justification, procedure, measures, and safeguards that will be implemented. The final objective of employing covert surveillance is an actual involvement of the police or other prosecution authorities for potential criminal investigation or civil legal proceedings that are being or have been issued, arising as a consequence of a criminal offence(s) having been allegedly committed.

Any case for covert surveillance must be justified prior to it being put in place and should only be done on a case-by-case basis. The following issues would need to be fully considered:

- What is the specific purpose(s) that the covert surveillance is trying to achieve? If it is to gather evidence, there must be a substantive factual circumstance(s) identifying an area of concern that needs to be further investigated by covert monitoring.
- Is this purpose a lawful objective? For example, are there any laws that prohibit such surveillance?
- Are there any alternative options to covert surveillance? For example, blocking access on work computers to social media or other non-work related sites?
- Is there any circumstantial evidence to support covert monitoring of an employee(s)? If so, how serious is the issue? There should be a risk analysis done as to the scale of inappropriate employee behaviour ranging from the most serious, such as a criminal offence of fraud/theft/gross negligence that could warrant an action for dismissal from employment to the less serious issues, such as timekeeping/personal emails, SMS or phone calls, that usually only warrant a manager's supervision.
- Relevant written company policies should be in place on workplace practices expected of employees.
- Under subsection 6(1) (f), an employer in their capacity as an organisation may use personal information if "the use of the personal information is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the organisation or in a third party to whom the personal information is disclosed". For this to occur, any use of personal information that is to be considered a "legitimate interest" must also consider the employment rights of the employee and their rights to privacy, data protection, fair procedures, etc.

Prior to any covert surveillance or monitoring, senior management should write a detailed policy that sets out the following:

- Full details as to why covert surveillance is required and why identified individuals are being targeted.

- Objective to be achieved: what type of evidence is being searched for and is it relevant, proportionate, and not excessive?
- How will this evidence be used? Will it be disclosed to an enforcement agency or is there potential for civil litigation?
- What happens to irrelevant information collected? A deletion policy must be in place for such information.
- Who in the organisation has overall responsibility for covert surveillance or monitoring and who else has authorised access to the information?
- It is recommended that an independent review of the information by a solicitor/legal adviser or trusted third party is carried out.
- It is recommended to set a short time period for surveillance or monitoring, i.e., one month or less if sufficient evidence is obtained in a shorter period.
- An organisation should undertake to present a copy of the full data set collected to each affected individual employee on completion of project together with a copy of the policy justifying it.

Retention periods

The length of time an employer can hold an employee's information is influenced by several factors; for example, there may be statutory obligations or industry guidelines that dictate the retention periods. Compliance with the principle of proportionality mandates that the information is retained for the least amount of time required to achieve the objective while ensuring that it is stored securely and is subsequently destroyed, deleted or erased securely at the appointed time.

(e) Employee rights

Employees as individuals have a number of specific rights under privacy PIPA to keep them informed and in control of the use(s) of their personal information. It is important that employers are aware of these rights as they have certain obligations and time frames to adhere to, should an employee wish to exercise any of these rights. While privacy rights are sourced under part 3 of PIPA, the most commonly exercised rights of individuals within the employment context are as follows:

Right to access personal information (section 17)

Section 17 of PIPA provides individuals/employees with the right to request access to their personal information. They are also entitled to receive the information set out under section 17 as part of their access request. Employers in their capacity as organisations must respond to these requests within the specific time frame, i.e., 45 days, or, where the nature of the request is complex, an additional 30 days, respectively.

Under subsection 20(1)(a), employers have up to 45 days from the date of receipt of the request to respond to an access request (section 17), a request to access medical records (section 18), and a request to correct, block, erase or destroy their information (section 19). This time frame can be extended by up to an additional 30 days, taking into consideration the complexity of the request. The employer must let the employee know promptly that an extension of time is required to deal with the request and they must state why.

If an employer engages the services of a third party and an employee makes an access request to the employer/organisation for access to a copy of the personal information the organisation holds on them, the responsibility for fulfilling the access requests rests with the organisation and not the third party.

Right to correction, blocking, erasure, and destruction (section 19)

Part 3 of PIPA provides for the rights of individuals/employees. Section 19 provides for the right of individuals/employees to have their inaccurate personal information corrected. This is in line with the principle under section 12 (integrity of personal information) that information shall be accurate and up to date to the extent necessary for the purposes of use; and that it is not kept for longer than is necessary for that use.

These rights exist, but they are not absolute. Employers can lawfully restrict the rights of employees/individuals depending on the circumstances of the request, such as the specified purpose and the effects of Section 10, Purpose limitation: in other words, when considering a request for correction, the request must be considered in line with considerations of the purposes for which the information was collected and used at the time; and/or in line with various provisions, such as sections 23-25. If an employer is relying on these provisions to restrict the rights of an employee who has sought to exercise their rights, they must set out which provision they rely upon and how compliance with PIPA would interfere with achieving the purpose in the specified exemption.