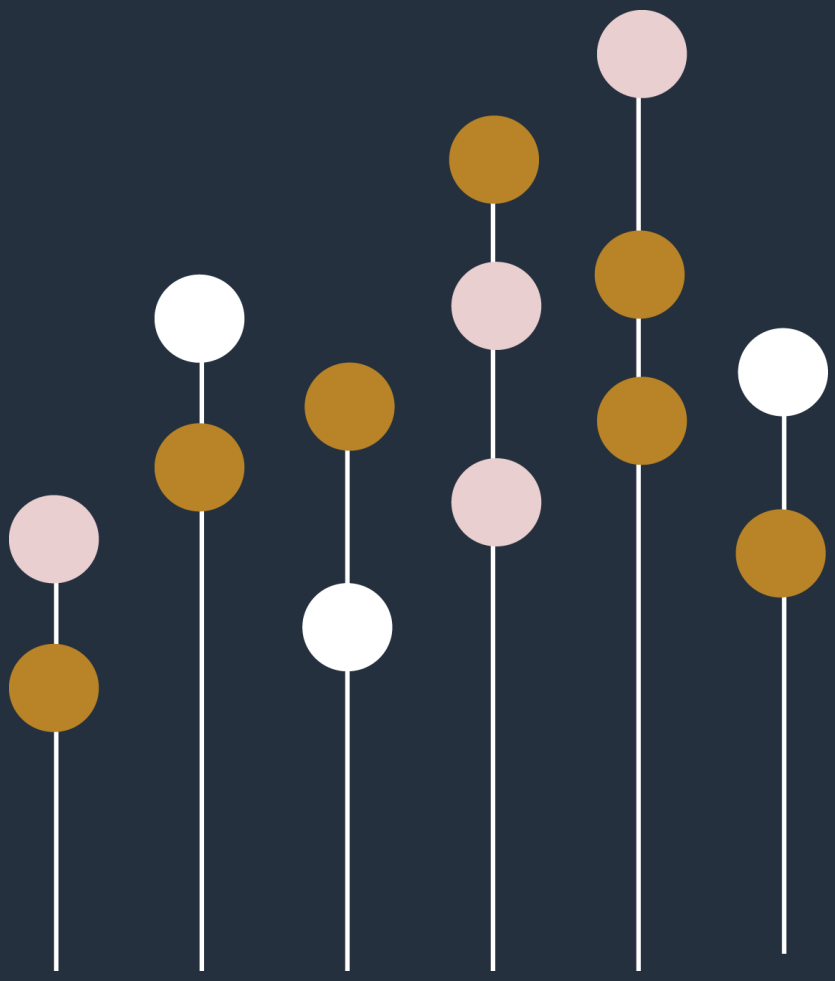
Card allowances: privacy considerations.



buddlefindlay.com

BUDDLE FINDLAY

Introduction

Employers often adopt card-based wellbeing allowances with the best intentions, aiming to support their employees' health and wellness. These allowances typically involve providing employees with prepaid cards that can be used at specific merchants, intended to cover various health or wellbeing related expenses. However, this seemingly beneficial approach can create legal risk. Employers may be able to see where these cards are being spent, leading to potential privacy breaches and loss of employee trust.

The ability to monitor where employees spend their allowances means that employers may be handling sensitive health data, such as visits to a sexual health clinic, dentist, or cancer specialist. This subjects them to Privacy Act 2020 (the **Privacy Act**) requirements they may not have realised. Without detailed policies, procedures, and clear communication with staff about how this data is handled, employers could find themselves in hot water. The lack of transparency and proper safeguards can lead to severe consequences, including financial penalties and damage to the company's reputation. This article highlights some of the major issues to be aware of, emphasising the importance of compliance with privacy laws.

The Privacy Act and your responsibilities

Many employers are unaware of the privacy issues associated with card-based allowances. Under the Privacy Act, employers must handle personal information with care, ensuring it is collected, used, disclosed, and stored in accordance with the Act. Card-based allowances can result in the collection of detailed spending data, including sensitive health information. This can easily extend beyond the initial intent of offering a wellbeing perk, potentially leading to misuse and unauthorised monitoring of employee behaviour.

Employers must be transparent about why they are collecting this information and how it will be used. Employees need to understand the purpose of data collection, who will have access to it, whether providing the information is compulsory or voluntary, and what will happen if they choose not to provide it. Additionally, reasonable safeguards must be in place to prevent misuse or unauthorised access to personal information. However, systems and policies governing access to this information may be inadequate, lacking proper oversight and security measures. Furthermore, personal information should not be retained longer than necessary. Finally, personal information should generally only be used and disclosed for the purpose it was collected, but detailed spending data can be repurposed, leading to potential misuse. This underscores the critical need for employers to develop comprehensive privacy policies and ensure ongoing compliance to avoid legal and financial repercussions.

Privacy principles and how they apply to card-based allowances

Card-based allowances may breach privacy regulations by not meeting the Privacy Act principles for handling personal information. Below, we outline these principles and show how card-based wellbeing allowances may fall short, exposing employers to legal and ethical risks.

Collection of information

Principle	Potential breach
Principle 1: You must only collect personal information if it is for a lawful purpose connected with your function or activities, and the information is necessary for that purpose.	The detailed visibility into employee spending which card-based allowances may allow may lead to the collection of sensitive health data that is not necessary for the purpose of the allowance. For instance, knowing that an employee spent their allowance at a sexual health clinic may not be relevant to the employer's function of providing a wellbeing perk.

Principle	Potential breach
Principle 2: Personal information should be collected directly from the person it is about, with their consent, or where it is not practicable or would undermine the purpose of collection.	Employees may not be explicitly informed or have given direct consent for the detailed tracking of their spending at specific merchants, leading to indirect collection of sensitive information without proper consent.
Principle 3: You must be open with an individual about why you are collecting personal information and what you are going to do with it. They need to understand why it's being collected, who will receive it, whether giving the information is compulsory or voluntary, and what will happen if the information isn't provided.	There may be a lack of transparency with employees about the extent of the monitoring or the information that an employer will collect. Without specific disclosures to employees about the level of visibility and the purposes for which the information will be used, employers risk being in breach of this principle.
Principle 4: Personal information must be collected in a way that is lawful and fair in the circumstances.	If an employee has not consented to the collection of their spending data with a card-based allowance, then any collection may not be fair.

Storage and security

Principle	Potential breach
Principle 5: You must ensure that there are safeguards in place that are reasonable in the circumstances to prevent loss, misuse, or disclosure of personal information. This includes having safeguards that only those who need to access and use the information can. The more sensitive the information (for example, health information), the more important it is to ensure that it is safeguarded.	Systems and policies governing who can access this information may be inadequate. Anyone with oversight of the cards or the account may have access to sensitive data without appropriate safeguards, which may lead to potential misuse or unauthorised access.

Access and correction

Principle	Potential breach
Principle 6: Individuals have a right to ask for access to their own personal information.	Employers must ensure that employees are made aware of their right to request information about themselves and that they are given access in accordance with the Act.
Principle 7: Individuals have a right to ask an organisation or business to correct information about them if they think it is wrong.	

Accuracy

Principle	Potential breach
Principle 8: You must check before using or disclosing personal information that it is accurate, up-to-date, complete, relevant, and not misleading.	The data collected through card-based allowances may not always be accurate or relevant, especially if it includes spending information that is not directly related to wellbeing.

Retention

Principle	Potential breach
Principle 9: You should not keep personal information for longer than it is required for the purpose it may lawfully be used.	Employers need to consider what information they are obtaining as part of any wellbeing policy and how long they need to retain it to meet their obligations under the law and not keep it for longer than is required.

Use and disclosure

Principle	Potential breach
Principles 10 and 11: You can generally only use and disclose personal information for the purpose it was collected. There are exceptions to this; however, they are limited in nature.	Detailed spending data collected through card-based allowances may be used for purposes beyond the original intent of providing a wellbeing perk, such as monitoring employee behaviour, leading to potential misuse of the information.

Disclosure outside of New Zealand

Principle	Potential breach
Principle 12: You can only send personal information to an organisation or people outside of New Zealand if you confirm several things about the receiving organisation. In summary that the receiving organisation: • Is subject to the Privacy Act because they do business in New Zealand • Will adequately protect the information • Is subject to privacy laws that provide comparable safeguards to the Privacy Act. If none of the above criteria apply, you can only make a cross-border disclosure with the permission of the person concerned.	Employers need to know whether they may be disclosing any personal information to people or organisations outside of New Zealand and if so, ensure they met the criteria set out in principle 12.

Unique identifies

Principle	Potential breach
Principle 13: You can only assign unique identifies to an individual when it is necessary to your function.	Unique identifies (i.e., individual numbers, references, or other forms of identification allocated to uniquely identify the person to the organisation) cannot be used unless it is necessary for your function.

Legal and financial ramifications

Non-compliance with the Privacy Act can result in financial penalties and damage to the company's reputation. Privacy breaches can lead to legal action and loss of trust among employees, complicating workplace morale and employee relations. The financial costs of defending privacy complaints and the potential for fines or awards as a result of a privacy breach should not be underestimated.

Ensuring compliance involves updating privacy policies, developing robust data protection procedures, and establishing clear internal communication lines for reporting and managing privacy issues. Failure to take these steps can result in legal and financial repercussions for employers.

Real-world examples of risk exposure

Below are illustrative scenarios that highlight the potential risks of using card-based wellbeing allowances. These examples demonstrate how such practices can lead to significant legal, ethical, and reputational issues for employers.

Monitoring without action or assumed monitoring without oversight

An employee uses their wellbeing allowance for therapy sessions or sensitive mental health support services, assuming or expecting that the employer is monitoring their spending and will notice if they need additional support. The employer monitors this spending but does not intervene or does not monitor the spending at all. The employee suffers a mental health crisis, expecting employer intervention that never comes. The employer could face a challenge from the employee that it failed to meet its health and safety obligations by not intervening and providing further support to the employee.

Perceived discrimination in termination

An employee is dismissed or made redundant and claims that the decision was influenced by their wellbeing spending on their card, such as seeing a cancer specialist or accessing mental health services. Regardless of whether the employer actually considered this data in its decision-making, the employee could argue that their termination was due to their health status, leading to legal disputes and reputational damage for the employer.

Unauthorised access to sensitive data

Spending data from card-based allowances, such as visits, and details of these visits, to a sexual health clinic, is accessible to various team members, including the finance team, HR team, and possibly other employees. This wide reach of sensitive information could constitute a significant breach of privacy. If unauthorised personnel access this data, it can lead to serious legal and ethical repercussions, including privacy breaches and potential legal action from affected employees.

Ethical and privacy concerns with card-based allowances

The detailed spending data collected through card-based allowances can easily be repurposed for uses beyond the initial intent of offering a wellbeing perk. This data may be leveraged to monitor employee behaviour, leading to potential misuse and unintended consequences. Even if such practices do not explicitly violate legal standards, they may raise significant ethical concerns, and may undermine the trust between employers and employees and expose organisations to both legal and reputational risks.

Conclusion

While card-based wellbeing allowances may seem convenient, there are privacy considerations that need to be considered. Employers should also consider whether there are alternative options available that better ensure confidentiality, target spending on genuine wellbeing support options, and comply with privacy laws.