# THE IMPACT OF DATA PRIVACY IN FRANCHISING

STEWART GERMANN LAW OFFICE
Lawyers, Notary Public

Stewart Lloyd Germann
B.Com, LL.B, FCIS, CFInstD, CFE, Notary Public
**Partner**

Khushbu Sundarji
BA, LL.B
**Partner**

Ground Floor, Princes Court
2 Princes Street, PO Box 1542
Auckland, New Zealand

Telephone 09 308 9925
Email stewart@germann.co.nz
Web www.germann.co.nz

When the Covid-19 pandemic hit the world in early 2020 the franchise industry was impacted just like anyone else. However, franchising has contributed immensely to economic recovery by providing considerable growth in relation to new systems development and appointing new franchisees in various industries.

The International Franchise Association's and FRANDATA 2022 Economic Outlook confirmed that "the total output generated by franchised establishments improved significantly by 16.3% to USD787.7 billion and was projected to grow to USD826.6 billion in 2022". That result is not out yet.

All parties collect a variety of information and in New Zealand there is a Privacy Act 2020 to comply with. There is information about franchise owners, employees, current customers, prospective customers, and clients.

Data privacy has become an increasingly important issue. In New Zealand the right to privacy is a fundamental human right. The modern threat to this is the increased collection and use of personal information which is essential to the operation of all Government and other agencies. Information is power. The citizens of New Zealand needed protection, so the Privacy Act 2020 was enacted. Legislation is complex, and some might say unnecessarily so.

The Act endeavours to control by statute the four ethical issues involved:

1. Privacy;
2. Accuracy;
3. Property;
4. Accessibility.

## 1. Privacy

What information about ourselves must we reveal to others?
Under what conditions and with what safeguards?
What information can we keep to ourselves and not be forced to reveal?

## 2. Accuracy

Who is responsible for the authenticity, fidelity and accuracy of information?
Who is to be held accountable for any errors in the information?
How is the aggrieved party to be compensated for any errors?

## 3. Property

Who owns the information?
What is a just and fair price for its exchange?
Who owns the way in which the information is disseminated?
How should access to this information be allocated?

## 4. Accessibility

What information does a person or an organisation have a right or a privilege to obtain? Under what conditions and with what safeguards?

### The Privacy Act

The essence of the Privacy Act is the identification of 13 information privacy principles which were established by the Organisation for Economic Cooperation and Development in Paris.

The 13 principles are as follows:

**Principle 1: Purpose of Collection of Personal Information.**

Personal Information shall not be collected by any agency unless it is collected for a lawful purpose connected with a function or activity of the agency and the collection of the information is necessary for that purpose.

**Principle 2: Source of Personal Information.**

Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.

**Principle 3: Collection of Information from an Individual.**

Where an agency collects personal information from an individual the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of:

(a) the fact that the information is being collected;

(b) the purpose for which the information is being collected;

(c) the intended recipients of the information;

(d) the name and address of the collection agency, and the holding agency;

(e) if the collection of the information is authorised or required by, or under, law. If so, under which particular law the collection of information is authorised or required, and whether or not the supplier of that information by that individual is voluntary or mandatory;

(f) the consequences, if any, for that individual if all or any part of the requested information is not provided;

(g) the rights of access to and correction of personal information provided by these principles.

**Principle 4: Manner of Collection of Information.**

Personal information shall not be collected by an agency by unlawful means or by means that, in the circumstances of the case, are unfair or intrude to an unreasonable extent upon the personal affairs of the individual concerned.

**Principle 5: Storage and Security of Personal Information.**

An agency that holds personal information shall ensure that the information is protected by security safeguards reasonable in the circumstances against loss, access, use, modification or disclosure except with the authority of the agency that holds the information and other misuse and that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

**Principle 6: Access to Personal Information.**

Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled to obtain from the agency confirmation of whether or not the agency holds such personal information, and to have access to that information to correct that information.

**Principle 7: Correction of Personal Information**.

Where an agency holds personal information, the individual concerned shall be entitled to request correction of the information and to request that there be attached to the information a statement of the correction sought but not made.

**Principle 8: Accuracy of Personal Information to be checked before use**.

An agency that holds personal information shall not use that information without taking such steps (if any) as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

**Principle 9: Agency not to use Personal Information for longer than necessary**.

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

**Principle 10: Limits on use of Personal Information**.

The agency holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds, that the source of the information is a publicly available publication or that the use of the information for that other purpose is authorised by the individual concerned, or that non-compliance is necessary, void, prejudiced to the maintenance of the law by any public sector agency, with the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue or for the conduct of proceedings before any Court of tribunal, or that the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to public health or safety, or the life and health of the individual concerned or another individual, or that the purpose for which the information is used is directly related to the purpose and connection with which the information was obtained or the information is used in a form in which the individual concerned is not identified or is used for statistical research purposes and will not be published and that the use of the information is in accordance with an authority granted under Section 54 of the Act.

**Principle 11: Limits on Disclosure of Personal Information**.

The agency that holds personal information shall not disclose the information to a person, body or agency unless the agency believes on reasonable grounds that the disclosure of the information is one of the purposes in connection with which the information was obtained, or is directly related to the purposes in connection with which the information was obtained or that the source of the information is a publicly available publication or that the disclosure is to the individual concerned, or that the disclosure is authorised by the individual concerned, or that non-compliance is necessary in order to avoid prejudice to the maintenance of law, for the enforcement of a law, for the protection of public revenue or the conduct of Court proceedings, that the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to public health, or public safety, or the life and health of the individual concerned, or that disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern, or that the information is to be used in a form in which the individual concerned is not identified, or is used for statistical or research purposes, or that the disclosure of the information is in accordance with an authority granted under Section 54 of the Act.

**Principle 12: Disclosure of Personal Information outside New Zealand.**

The agency can only send personal information to someone overseas if the information will be adequately protected. For example:

- the receiving person is subject to the New Zealand Privacy Act because they do business in New Zealand;
- the information is going to a place with comparable privacy safeguards to New Zealand;
- the receiving person has agreed to adequately protect the information – through model contract clauses, etc.

If there are no adequate protections in place, the agency can only send personal information overseas if the individual concerned gives the agency express permission, unless the purpose is to uphold or enforce the law or to avoid endangering someone's health or safety.

**Principle 13: Unique Identifiers.**

An Agency shall not assign a unique identifier to an individual unless the assignment of the identifier is necessary to enable the Agency to carry out any one or more of its functions efficiently. An Agency which assigns a unique identifier such as a pin number which identifies an individual other than their name may only do so if this step is necessary to carry on one or more of its functions efficiently, and the Agency has taken all reasonable steps to clearly establish the identity of that individual.

It is very important for franchise parties to prevent data privacy violations. Franchisees will collect information pertaining to their employees, customers and suppliers. Franchisees must evaluate the information and how to protect it and they should conduct data mapping which is an internal audit process which allows the franchisee to determine what types of personal data it is receiving, where it is being stored, why it is being collected, and how long the franchisee intends on keeping the data.

Franchisors must take an active role in the protection of stored data and compliance with regulations. In the unfortunate event of a data breach or public violation of data privacy regulations, there will be a direct harm to the brand regardless of who is responsible for the violation. Data breaches can result in significant costs for the franchisor. For example, in 2021 IBM found that an average cost of a data breach was USD4.24 million which went up 10% compared to 2020.

Franchisors must remain cautious of potentially non-compliant activities by franchisees. They must ensure that all franchisees conduct their businesses to high standards to ensure compliance with the laws. While most franchise agreements do not provide for unilateral changes, some franchisors have addressed changing standards by way of amendments to the operations manual. Franchisors can require written confirmation from franchisees that they have complied with any changes to data collection and data privacy laws and require that any changes will replace a current data protection plan.

In conclusion, franchisors and franchisees must operate their businesses in compliance with the expanding data privacy legislation and always take appropriate steps to ensure compliance.

**Stewart Germann**
Franchising Lawyer
Auckland
stewart@germann.co.nz
www.germann.co.nz

March 2023