Office of the
Information &
Privacy Commissioner
for British Columbia

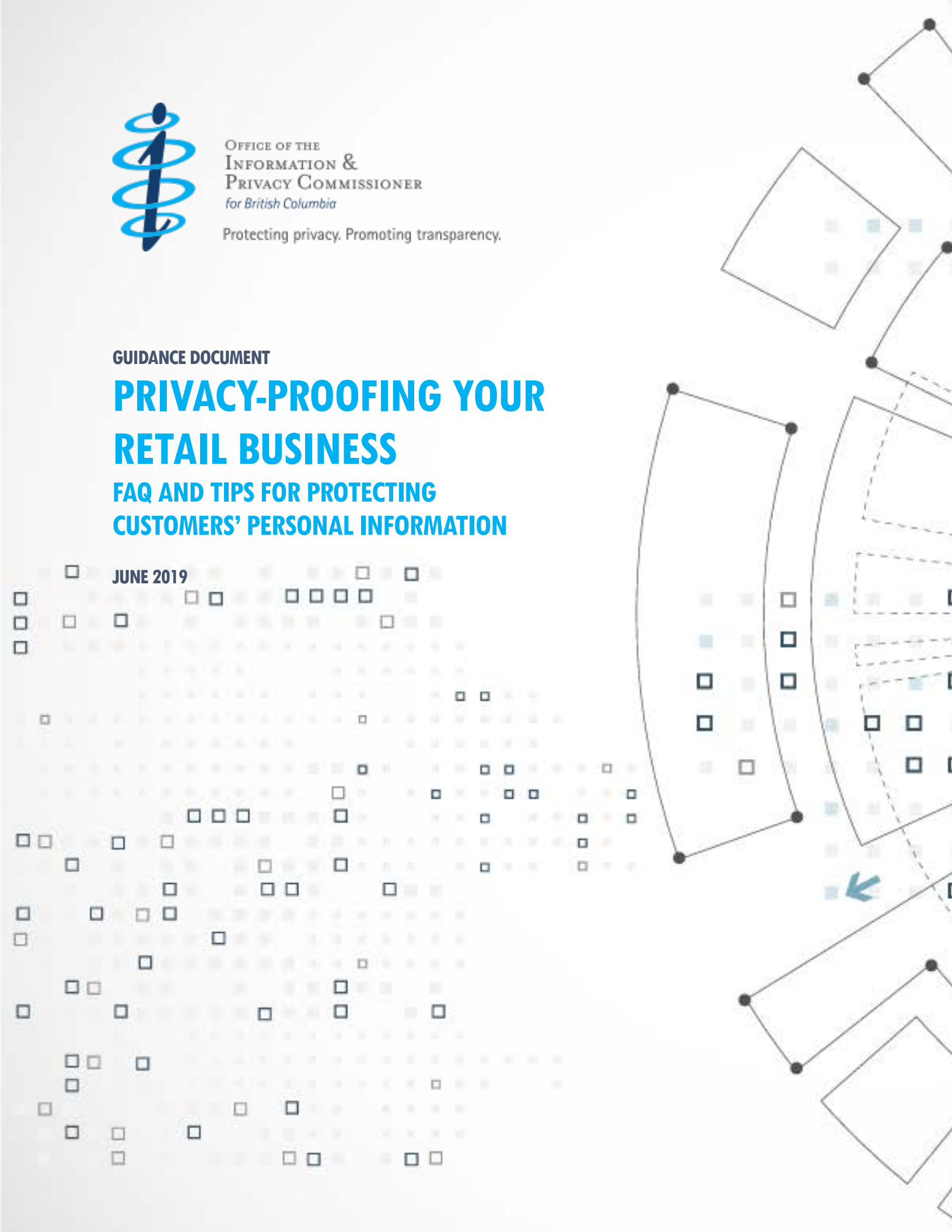
Protecting privacy. Promoting transparency.

GUIDANCE DOCUMENT

PRIVACY-PROOFING YOUR RETAIL BUSINESS

FAQ AND TIPS FOR PROTECTING CUSTOMERS' PERSONAL INFORMATION

JUNE 2019



CONTENTS

PURPOSE OF THIS GUIDANCE DOCUMENT

The *Personal Information Protection Act* (PIPA) applies to any private sector organization that collects, uses, or discloses the personal information of individuals in BC, including retail businesses.[1]

This guidance document aims to help retail businesses understand their obligations under PIPA and outlines best practices.[2]

PERSONAL INFORMATION

PIPA defines personal information as "information about an identifiable individual." This is a broad definition that can include name, date of birth, phone number, address, email address, driver's license number, physical description, image, voice or biometric template[3], social insurance number, financial information (such as a credit card number), and an individual customer's purchase and return records. PIPA excludes business contact and work product information from this definition.

PIPA sets out the rules for the collection, use, and disclosure of personal information. The questions and answers below illustrate how the legislation applies to situations commonly faced by retail organizations in their customer transactions.

---

[1] The scope of this guidance document concerns protection of customer personal information. For guidance on protection of employee personal information, please see OIPC guidance document Employee Privacy Rights.
[2] This document is limited to privacy considerations; retail organizations have many other legal obligations, such as those under consumer protection laws and employment laws.
[3] A biometric template is a digital reference of an individual's physical characteristics, such as a biometric template of an individual's face captured by facial recognition technology.

COLLECTION OF PERSONAL INFORMATION

1. What personal information can we collect from customers?

Limit the information you collect to only what a reasonable person would consider appropriate in the circumstances to complete the purchase of the product or service you are providing.[4]

2. What do we do if we want to verify a customer's identity to protect against fraud?

If a customer pays cash, it is not reasonable to ask for proof of identity because you do not require that information to provide the product or service.[5] If a customer offers payment by other means, you may ask to see identification, such as a driver's license, to confirm the individual's identity. However, you may not record that information unless having it recorded is required for the product or service you are providing.[6]

3. When can we ask a customer for a social insurance number (SIN)?

The SIN is an identification number created under federal law to administer certain government laws and programs, such as the Income Tax Act and the Canada Pension Plan. You can only collect an individual's SIN number with consent if it is reasonable in the circumstances.[7] You should keep in mind that inappropriate use of the SIN poses serious privacy risks for individuals.

4. Can we ask customers for their phone numbers, email addresses, or postal codes?

Yes, as long as it is for a purpose that a reasonable person would consider appropriate and you obtain consent (unless this is not required under PIPA.[8]) For example, if you offer an electronic newsletter, you may collect subscribers' email addresses; however, you cannot require a customer to provide this information as a condition of sale unless it is necessary for the transaction.[9]

---

[4] PIPA s. 11
[5] PIPA s. 7(2)
[6] PIPA s. 7(2)
[7] PIPA s. 11
[8] Section 12 of PIPA sets out circumstances where organizations can collect personal information about an individual without consent.
[9] PIPA s. 7(2)

5. When can we use video surveillance?

If you are considering the use of video surveillance, it is important to note that capturing an individual's image, voice, or biometric template[10] constitutes a collection of personal information. You may only collect personal information via video surveillance if it is reasonable in the circumstances. [11] You may want to consider less intrusive measures before installing video surveillance. However, if you decide to use it, you must notify individuals of the purpose for the collection at the time of or before the camera collects their personal information.[12] Retail businesses can notify customers using clear signage that they can read before they elect to enter the premises and the camera collects their personal information. Cameras must not capture footage beyond your property.[13]

Individuals also have the right to request a copy of their own personal information, which could include video surveillance footage. You must be prepared to locate the requested information and respond to these requests. [14] If you provide a copy, you must also be prepared to remove the personal information of other individuals in the video footage.[15]

NOTICE AND CONSENT

6. Can we record a customer's personal information to speed up their future purchases or later notify them of attractive offers?

Yes, as long as you obtain consent and clearly explain why you are collecting the information, exactly how you will use it, and permit customers to decline this service.[16]

7. Does this mean we always have to explain to customers why we are collecting their personal information and how we are planning to use it or disclose it to other organizations and get their consent to do so?

Yes, unless the purpose for collection, use, or disclosure would be obvious to a reasonable person and the customer voluntarily provides the information for that purpose. This constitutes implicit consent.[17]

---

[10] Biometrics templates in video surveillance refers to biometric images of the face, gait or iris, for example, captured using surveillance videos.
[11] PIPA s. 11
[12] PIPA s. 10
[13] This is because PIPA generally requires consent before personal information is collected by surveillance.
[14] PIPA s. 23(1)(a)
[15] PIPA s. 23(4)(c)
[16] PIPA s. 7(2)
[17] PIPA s. 8(1)

8. If we hold a draw for a weekend getaway to a ski resort and ask customers to provide their names, addresses, and phone numbers to enter, wouldn't it be obvious we are planning to use that information for marketing purposes?

It might seem obvious to some customers but not to others. Be transparent about how you are going to use the information. In this case, you could include an explanatory note on the entry form stating that you will use their information for marketing purposes.[18]

9. Do we have to get customers' consent in writing?

PIPA does not require written consent, but written consent or opt-in consent may better protect you if a customer challenges consent.

Please see the Office of the Privacy and Information Commissioner for BC's (OIPC) guidance document Obtaining Meaningful Consent.

10. Can a customer withdraw consent?

A customer can withdraw or change their consent by giving you reasonable notice.[19] You must let the customer know the consequences of withdrawing or changing consent.[20]

11. If we offer discounts to customers who join our rewards program, would it be considered reasonable for us to track their purchases and notify them of special offers?

It would only be considered reasonable if you clearly explain your intention to do so when they register for the program and you obtain their consent. Under PIPA, organizations cannot require a customer to consent to the collection, use, or disclosure of their personal information as a condition of supplying the customer with a product or service unless their personal information is necessary to supply that product or service.[21]

ACCESS AND CORRECTION

12. What is a privacy policy and how do we develop one?

A privacy policy is an effective way to explain how you will put PIPA into effect with respect to personal information that you collect, use, and disclose. No matter how small your

[18] PIPA s. 10(1)
[19] PIPA s. 9(1)
[20] PIPA s. 9(2)
[21] PIPA s. 7(2)

organization, you are legally obligated to develop policies and practices to meet your responsibilities under PIPA.[22]

Please see OIPC guidance document Developing a Privacy Policy under PIPA.

13. What happens if a customer asks to see our privacy policy and talk to our privacy officer?

If requested, you must be prepared to provide information about your policies and practices, including the complaint process. You also must designate a privacy officer – an employee who is responsible for ensuring you comply with PIPA – and provide the employee's position name or title and contact information, as requested.[23]

14. What happens if a customer asks for a copy of all of his or her personal information? Isn't it ours once we have it?

Under PIPA, individuals have a right to request access to their personal information and you must respond no later than 30 days after receiving the applicant's request, subject to an extension.[24] PIPA states that organizations may charge a *minimal* fee to provide individuals with access to their information.[25] In some cases, PIPA either authorizes or requires you to withhold personal information. For example, you can only disclose the personal information of the individual making the request, not that of others.[26]

15. What do we do if a customer wants us to correct his or her personal information?

Under PIPA, you are required to make reasonable efforts to ensure that the personal information you collect is accurate and complete, if you are likely to use the personal information in decisions that affect individuals or disclose it to another organization.[27] You must also make reasonable arrangements to ensure that the personal information you collect, use, or disclose is accurate and complete.

So yes, individuals may request that you correct any errors or omissions in their personal information that is under your organization's control.[28] If you are satisfied that an individual's request for correction is reasonable, you must correct the information. You must also send the corrected information to organizations you disclosed that information to during the year before the date you made the correction.

---

[22] PIPA s. 5
[23] PIPA s. 4
[24] PIPA ss. 23,29,31
[25] PIPA s. 32
[26] PIPA s. 23(4)(c)
[27] PIPA s. 33
[28] PIPA s. 24(1)

If you are not satisfied that the request is reasonable, you must annotate the information. Note that the correction was requested but not made.[29]

16. What happens if a customer wants to make a complaint?

A customer must send a written request to your organization.[30] If you do not respond in 30 days or the complainant is not satisfied with your response, a customer can complain to the OIPC, requesting a review or making a complaint to the Commissioner.[31] If the request for review or complaint is accepted, the OIPC will assign it to an investigator who will review the evidence and try to mediate the dispute or make findings. If mediation is unsuccessful, the file may proceed to inquiry for adjudication, which will result in a legally binding order.[32]

SAFEGUARDS AND RETENTION

17. What security measures do we need to protect customers' personal information?

You must protect all personal information in your custody or under your control by making reasonable security arrangements to prevent unauthorized access, collection, use, copying, modification or disposal, or similar risks.[33] The extent of your security should align with the sensitivity of the personal information in your custody or under your control.[34]

Please see OIPC Guidance Document Securing Personal Information: A Self-Assessment Tool for Organizations.

18. What responsibility do we have for the privacy practices of organizations to which we disclose our customers' personal information?

You are responsible for personal information that is directly under your control, which can include personal information not in your custody. You should ensure that any other organizations with which you share your customers' personal information also comply with PIPA. In order to meet your organization's obligations under PIPA, it is considered a best practice to have contractual provisions that detail these expectations and ensure you can monitor how the other organization is protecting the personal information your organization collects.

---

[29] PIPA s. 24(2),(3)
[30] PIPA s. 27
[31] PIPA ss. 46,47
[32] PIPA s. 50
[33] PIPA s. 34
[34] Investigation Report F12-02

19. How long should we keep personal information after collecting it?

PIPA requires you to destroy documents containing personal information, or remove the means by which the personal information can be associated with particular individuals, once the purpose for which the personal information was collected is no longer being served by retention, and retention is no longer necessary for legal or business purposes.[35]

If you have used customer personal information to make a decision that directly affects the customer, you must keep it for at least a year after making the decision so the customer has a reasonable opportunity to access it.[36]

20. How should we dispose of documents containing personal information?

Whether your documents for disposal are paper or electronic, on hard drives, surveillance tapes, or any other medium, you have a responsibility to ensure your practices for properly disposing of personal information in your custody meet your safeguard obligations under PIPA.[37] A cross-shredder or using bonded shredding company is a best practice if you are disposing of paper. Ensure you delete or destroy electronic records so that personal information cannot be recovered.

21. What should we do if a customer's personal information is improperly used or disclosed?

Depending on the risk of unauthorized access and use, you should immediately seek to contain the breach and report it to your organization's privacy officer. Next steps will likely include evaluating the risks, deciding whether to notify affected individuals, and implementing solutions to prevent future breaches. You should have procedures in place for responding to suspected breaches.[38] You may also contact the OIPC for information on how to manage the breach.

Please see OIPC guidance document Privacy Breaches: Tools and Resources

RESOURCES FOR FURTHER INFORMATION

Visit www.oipc.bc.ca/resources/guidance-documents/ for further guidance on how to comply with PIPA.

[35] PIPA s. 35(2)
[36] PIPA s. 35(1)
[37] PIPA ss. 34,35(2)

These guidelines are for information purposes only and do not constitute a decision or finding by the Office of the Information and Privacy Commissioner for British Columbia. These guidelines do not affect the powers, duties, or functions of the Information and Privacy Commissioner regarding any complaint, investigation, or other matter under FIPPA or PIPA.

PO Box 9038 Stn. Prov. Govt. Victoria BC V8W 9A4 | 250-387-5629 | Toll free in BC: 1-800-663-7867
info@oipc.bc.ca | oipc.bc.ca | @BCInfoPrivacy

OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.