MORTGAGE BROKERS

PIPEDA and You

Since mortgage brokers and their agents regularly collect, use and disclose personal information during the course of their work, they have privacy legislation compliance obligations.

For mortgage brokers and their agents, compliance with privacy legislation is not only essential, but it can help build an atmosphere of trust with clients, improve organizational reputability, and strengthen business operations.

The Personal Information Protection and Electronic Documents Act (PIPEDA) is Canada's federal privacy legislation that applies to organizations engaged in commercial activities across the country, except in provinces that have their own private sector privacy laws. Even in these provinces, PIPEDA continues to apply to the federally-regulated private sector and to personal information in inter-provincial and international transactions.

The Office of the Privacy Commissioner of Canada (OPC) audited a number of mortgage brokers and released the audit report in June 2010. Based on this audit, we have developed a number of best practices for brokers and their agents with respect to their information-handling practices, among these are:

Have A Privacy Plan And Be Open About Your Practices: Private sector privacy legislation requires organizations to build privacy policies that outline how they collect, use and disclose their customers' personal information. In the OPC's Privacy Guide For Small Businesses, there are a number of tips to help you develop and build a privacy policy.

Your privacy policy should be made available to your clients – make it available on your website and available in print for clients without internet access. As well, your clients should know who in your organization they can contact if they have questions regarding their personal information.

Collect Only What You Need: Your privacy plan should identify that you limit the collection of personal information for specified purposes – and your business practices should reflect that! For example, a Social Insurance Number (SIN) should not be used as a general identifier, and its collection, use and disclosure should be limited to its legislated purposes only.

Obtain Your Client's Consent: You should obtain and document your client's express consent before obtaining credit reports and providing information to lenders. Individuals need to know – in a meaningful way – how their personal information is going to be handled. This is especially true if their personal information is used for secondary purposes such as marketing, in which case express consent must be obtained with the ability for individuals to opt-out.

Limit Access to Personal Information on a "Need-To-Know" Basis: Having your client's personal information is like having their wallet – and should be protected as such.Develop policies that limit access to personal information on a "need-to-know" basis. For example, when it comes to credit reports, only those individuals who need them should have access to them.

Safeguard Personal Information: A variety of physical and technological methods can be used to safeguard personal information, these include: locked filing cabinets, alarm systems, secured premises, computer passwords and encryption. Files stored in the open, such as in open boxes in hallways or left unattended in easily accessible areas, could be accessed by unauthorized individuals and be the cause of a data breach.

As well, agents who take files home – either electronic or paper files – should ensure that they have a safe place in which to store them, otherwise, files should not be removed from the brokers' premises.

Keep Only What You Need For As Long As Is Required: You should only keep information for as long as is required and consideration must be given to any legislative requirements – federal or provincial. As well, make sure your clients are aware of your retention requirements, policies and procedures. Your policies and procedures should be periodically reviewed to ensure that your operations and practices mirror what you say you are doing.

A retention policy should also demonstrate that personal information is securely disposed of in a reasonable time. For example, if mortgage applications and credit reports are no longer required and your policy includes shredding, it is recommended that a cross-cut shredder is used.

Develop A Training Plan: PIPEDA requires that employees understand their role in implementing privacy policies. As such, brokers and their agents need to be aware of their privacy responsibilities and company-specific privacy practices.

Training should take place before agents are in a position to handle personal information and ideally refresher training should be given on a regular basis.

Develop a Breach Response Plan: A privacy breach occurs when there is unauthorized access to, or collection, use, or disclosure of, personal information. It can happen when customer data is lost on a USB stick, stolen via a cyber attack on your IT systems, or mistakenly e-mailed, faxed or mailed to a party who is not authorized to have the information.

It is important to develop a clear set of procedures with respect to handling any unauthorized access or loss of personal information – and tying this to your business continuity planning would be a good idea. Your plans and procedures should take into consideration:

(1) breach containment and preliminary assessment activities;
(2) evaluation of the risks associated with the breach;
(3) a notification strategy; and
(4) steps needed to prevent future breaches.

The OPC has developed a number of online resources and tools specifically to help private sector organizations subject to PIPEDA understand their privacy obligations.

We encourage you to access these documents from the OPC's Information for Private Sector Organizations webpage.

Please also visit the OPC's homepage for additional information. **www.priv.gc.ca.**