Pennsylvania Association of
REALTORS®
REALTOR® **The Voice for Real Estate® in Pennsylvania**

PENNSYLVANIA DATA SECURITY LAWS

BREACH OF PERSONAL INFORMATION NOTIFICATION ACT

Q: **Does Pennsylvania have any law on data security?**

A: There are two laws addressing data security in Pennsylvania. Pennsylvania's Breach of Personal Information Notification Act, (BPINA), otherwise known as Act 94 of 2005, and the Privacy of Social Security Numbers Act, otherwise known as Act 60 of 2006.

Q: **What is the BPINA privacy law?**

A: This law applies to any "entity that maintains, stores or manages computerized data that includes personal information" on a Pennsylvania resident and requires the collecting entity to provide notification to those residents who are affected by a security breach of the computerized data.

Q: **When did the BPINA become law?**

A: The Act was signed into law in December, 2005 and became effective on June 20, 2006.

Q: **Does the BPINA apply to real estate brokers and agents?**

A: Yes. Any individual or business doing business in the state is covered by the Act, as is any governmental entity.

Q: **How do I determine if I am working with a Pennsylvania resident?**

A: A Pennsylvania resident is a natural individual whose principal mailing address, as reflected in the computerized data that is stored, maintained, or managed by an entity is in the Commonwealth of Pennsylvania.

Q: **What "personal information" is covered by the Act?**

A: Personal information is any data record that links to a person's first and last name, or their first initial and last name, to their:

1. Social Security Number;
2. Driver's license number or a personal identification card issued in lieu of a driver's license; or
3. Financial account number, credit or debit card numbers in combination with any security access code or password that permits access to the financial account.

Q: **Some of this personal information may be necessary to a real estate transaction. Does the law say I can't get this information from clients?**

A: The BPINA doesn't restrict the collection of any personal data, but collection and use is limited to the "good faith acquisition by an employee or agent of an entity if used for a purpose that is the lawful purpose of the entity and not subject to further unauthorized disclosure or use." If personal information is necessary for a transaction you can still collect it, but brokers may need to pay closer attention to how the data is stored and secured. If there is not an absolute need for certain information, or there is a need to get the information but not to store it, brokers may want to consider changing their practices to reflect this.

Q: **What sorts of data storage would be considered a "computerized data?"**

A: The Act does not contain a definition of the phrase "computerized data," but a common-sense reading of the term suggests that any personal information stored electronically would probably qualify. Data qualifying as "personal information" maintained in the following types of applications would probably be covered under the Act:

-- Contact management systems (Top Producer, ACT!, or a proprietary brokerage system, for example)
-- Electronic forms (RealFAST, ZipForm, Trueforms or Instanet)
-- Excel spreadsheet
-- Scanned documents
-- E-mail messages

Q: **What is a breach of the security of the system?**

A: A breach is the unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity.

Q: **How do I know if the breach materially compromises personal information?**

A: To materially compromise the security or confidentiality of personal information, the entity must reasonably believe the breach has caused or will cause loss or injury to any resident of Pennsylvania. As a general matter, if there has been a breach of security it is probably better to err on the side of caution and make the required notifications.

Q: **When is notification required?**

A: Notification must be made without unreasonable delay after determining the scope of the breach and integrity of the data system has been restored.

Q: **What is considered notice?**

A: There are 4 primary ways to provide notice to a consumer in the event of a breach or a suspected breach. Notification may be made by *any* of the methods.

1. Written notice to the last known home address.
2. Telephonic notice if there is a reasonable belief the consumer will receive it and only when the notice is given in a “clear and conspicuous manner.” Clear and conspicuous manner is a message that describes the incident in general terms. However, when using this method, the resident must not be required to provide personal information, but instead should be given a telephone number to call or Internet website to visit for further information or assistance.
3. Email notice is allowed when there is a prior business relationship and a valid email exists for the consumer.
4. Substitute notice is allowable when the cost of providing notice exceeds $100,000 or the breach affects a number of consumers that exceeds 175,000 or the entity does not have sufficient contact information to make notification. Substitute notice may be by any of the following methods:
   a. Email notice if an email address exists for the resident; or
   b. Conspicuous posting of notice on the entity’s website, or
   c. Notification via a major statewide media.

Q: **Is a record destroying company considered a covered business or entity under BPINA?**

A: Yes, a record destroying company must comply with BPINA.

Q: What is a vendor under BPINA?

A: A vendor is a third party who maintains, stores or manages computerized data on behalf of an entity. For example, if you use an online forms provider that stores data on a server, that forms provider would be considered to be a “vendor.”

Q: **Is there a notification requirement for vendors storing data for me?**

A: Yes. Any breach of the security of computerized data maintained by the vendor triggers a requirement that the vendor report that breach to the entity for which it is maintaining the data. It is then up to the entity to decide if the breach was sufficient to require the collecting entity to notify the consumers.

For example, if a broker is using the online forms product of XYZ Forms Company and keeps a customer’s name and social security number in the database, the broker is a collecting entity and XYZ is a vendor. If XYZ Forms has a security breach of any type, XYZ must immediately notify broker of the breach. Broker is then responsible for determining whether the breach “has caused or will cause loss or injury to any resident of Pennsylvania.” If so, the broker is now responsible for notifying all individuals from whom he collected personal information about the breach. If XYZ is storing data from 100 broker clients in Pennsylvania, the vendor would have to notify each of the brokers and each broker would be responsible for notifying its own customers.

Q: **Do I have to report the breach to a credit reporting company?**

A: You must the breach to a credit reporting company when a breach of data security affects more than 1,000 Pennsylvania residents. This notification must also be made without unreasonable delay.

Q: **How many credit reporting agencies must I report to when breach of data security occurs?**

A: You must make a report to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

Q: **Are there any exemptions under BPINA**?

A: The Act does not apply where the personal information is completely or partially redacted. A limited exemption applies when the data is encrypted. If the encrypted data is accessed in an unencrypted form, or if the security breach involves the breach or possible breach of the encryption key or password, notification must still be provided.

Q: **What is redaction of personal information?**

A: Redaction of personal information is the alteration or truncation of data elements such that no more than the last four digits of a Social Security number, driver's license number, state identification card number or account number is accessible as part of a consumer's data. For example, the Social Security Number field might read "XXX-XX-3069" where the data has been redacted.

If the data is redacted, the notification provisions of this Act do not apply. Note that the redaction must prevent the data from being accessed, not just prevent it from being seen on screen. That is, if the screen shows "XXX-XX-3069" but the underlying database still has the entire 8 digit number available for someone who knows how to obtain it, the information would not be considered to be redacted (although it might have been encrypted, *see* below).

Q: **What is encrypted information?**

A: The technical definition of encryption is "an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." In short, encryption is a process that scrambles data unless the user has a password or other key that unscrambles the data to make it useful.

For example, a data program might be written to automatically substitute the letter "X" for the first 5 digits of any Social Security Number if the information is viewed without a password. Once the user supplies the appropriate password, the entire number could be viewed.

Q: **Is a REALTOR® association exempt from BPINA?**

A: No. If the Association or Board is maintaining computerized data containing the names of members along with any of the three data elements then the association is not exempt from BPINA. The same exemptions for encrypted and redacted data apply.

Q: **What is the penalty for not notifying a consumer?**

A: The Office of the Attorney General has the exclusive authority to bring action under the Unfair Trade Practices and Consumer Protection Law for violations occurring under BPINA.