

# NEW PRIVACY LAWS REQUIRE CHANGE IN OPERATING PROCEDURES FOR SELF-STORAGE FACILITIES

by Connie N. Heyer, TMSA Legal Counsel

**T**he hottest topic, next to taxes, in the regular 2005 legislative session was privacy and identity theft. Many bills were introduced on this topic, and three bills ended up passing and will become effective September 1, 2005. All three of these bills will affect most businesses in the state, including self-service storage facilities.

This article will provide a summary of the end result of the three bills – how these three new laws will affect your self-storage business practices and what changes our members need to make in their operations.

*What is considered “Sensitive Personal Information” (SPI), and what are the document disposal requirements for SPI?* The new privacy laws will affect your document disposal practices in the future. The new laws are effective September 1, 2005 and any business record you dispose of on or after that date, if it contains the information described below, must be shredded, burned, or the SPI must be erased or otherwise made unreadable.



The following information is the sensitive personal information (SPI) that triggers the shredding or erasing requirements: A person's *first name or first initial, and last name, in conjunction with any of the following:*

- Driver's license number
- Date of birth
- Social Security number or government identification number
- Mother's maiden name
- Unique biometric data (fingerprint, voice recording, etc.)
- Unique electronic identification number (like a routing code for wiring funds)
- Debit or credit card number
- Financial institution account number or other financial information (such as a credit report)

Before disposing of any of your business records containing SPI, you must make the SPI on the record unreadable (darken it out with a pen so that it is unreadable, or otherwise make it unreadable, or shred or burn the document). Several TMSA forms contain SPI, so after September 1, 2005, you will need to shred the forms or otherwise make the personal information unreadable before disposing of them.

Some of the TMSA forms containing SPI include (all page numbers are from the 2004-2005 TMSA Goldbook): the first page of the TMSA lease (Self-Service Storage Rental Agreement), page 382-383; TMSA Change of Address, Telephone Number or Other Tenant Information on page 390; Authorization and/or Release by Tenant on page 393; Notice to Issuer of Returned Check on page 394; and Tenant Information Sheet on page 399. This is a sampling and not an all-inclusive list of forms potentially containing SPI, and you should check your own forms also to see if they contain the information in the SPI list above. It is recommended that if you are hiring a shredding company to shred your business records, you require them to shred your records on site — best not to let them take the records unshredded and trust that they will shred them before disposing of them.

The penalties for failing to properly dispose of a business record containing SPI are, under one of the new laws, \$500 per record, and under another new law, a fine of between \$2,000 and \$50,000 per violation. Hopefully next session the legislature will clean up these conflicting and duplicative new laws, but regardless, the penalties for failure to properly dispose of records containing SPI are very high.

## Adopting a Privacy Policy

The new laws require you, in all cases, to implement and maintain reasonable procedures, including taking any appropriate corrective action, to safeguard SPI contained in your business records. If you require a Social Security number as a condition of leasing to a tenant, then you *must* adopt a privacy policy, make the privacy policy available to the tenant, and this privacy policy must maintain the confidentiality and security of the Social Security number. Probably the best way to make sure that you are complying with all “safeguarding” requirements is to adopt a privacy policy, even if you do not require Social Security numbers as a condition of leasing. Your privacy policy should include the following components (and *must* include these components if you require Social Security numbers from your tenants):

- How personal information is collected
- How and when the personal information is used
- How personal information is protected
- Who has access to the personal information
- How the personal information is disposed of

*Continued on next page*

You are only *required* to adopt a privacy policy if you require your tenant to disclose a social security number, but regardless it makes sense to adopt a privacy policy in order to make sure you satisfy the general requirements of “maintaining reasonable procedures” to safeguard this information. You are not required to give each tenant a copy of the privacy policy. You must simply “make it available” to your tenants (and employees, and whoever else your business maintains records on). If the tenants ask, you need to give them a copy of the policy. You may also post a copy of the privacy policy in the office. Anything that “makes available” your privacy policy will pass muster under the law.

### **Security Breaches**

You are required to take appropriate corrective action in the event of a security breach where someone has, without authorization, accessed files that contain SPI. “Corrective action” is not defined, but in all likelihood it would be interpreted to require tenant notification if his SPI may have been accessed without your authorization. Additionally, if your computerized data includes SPI and there is a breach of your computer system security, after discovering or receiving notification of the breach, you are specifically required to, as quickly as possible, give written notice to any person in your computer system whose SPI may have been accessed without authorization. If the number of people who you will have to notify is more than 10,000 people, you must also promptly notify all consumer reporting agencies that maintain files on consumers on a nationwide basis, and notify them of the timing, distribution and content of your notices to your tenants.

Due to this requirement and the potential for security breaches, it would make sense to purge any unneeded paper files containing SPI and electronically-stored SPI in your system. TMSA legal counsel recommends that all tenant records be retained (or a copy of them retained) if possible for four years from the date of lease termination, as four years is the statute of limitations for breach of contract action. There is no timeframe for record retention required by law. It is a case-by-case decision for each business owner to make.

### **Summary**

In summary, as of September 1, 2005, before disposing of any records that contain sensitive personal information (as defined above), you will need to shred them, or otherwise make the SPI on them unreadable (black out the SPI, burn the whole document – whatever will result in SPI being

unreadable). If you require a tenant’s Social Security number as a condition of leasing, you must adopt a privacy policy that contains the requirements of the new state law, and you must make that privacy policy available to your tenants. If you do not require disclosure of a Social Security number, you must still “maintain reasonable procedures” for safeguarding sensitive personal information that you have in your files.

If your paper files are accessed without your authorization, you must take “appropriate corrective action.” If your computer files containing sensitive personal information are accessed without your permission, as quickly as possible after you discover the security breach, you must provide written notice to any tenant or individual whose sensitive personal information might have been accessed.

A sample privacy policy that complies with the state law requirements is printed below. Owners are welcome to make their own privacy policy as long as it complies with all of the state law requisites listed in the “Adopting a Privacy Policy” summary above. More information about these statutes will be in the 2006-2007 *Goldbook*© including copies of the statutes themselves. You may access any of these bills (new laws) and print out copies of them by visiting [www.capitol.state.tx.us](http://www.capitol.state.tx.us) and going to the “Legislation” section. The bill numbers are: House Bill 698 (dealing with record disposal); Senate Bill 122 (dealing with record disposal, record safeguarding, and security breaches); and House Bill 1130 (dealing with privacy policies.) These bills became law in the 79<sup>th</sup> Regular Legislative Session.

### **SAMPLE PRIVACY POLICY XYZ SELF-SERVICE STORAGE**

Our privacy policy will be made available to any of our tenants or employees upon request as required by state statute. State statutes have defined certain “sensitive personal information,” including driver’s license numbers, dates of birth, and Social Security numbers, and we have adopted this privacy policy to help ensure the security of this sensitive personal information. Our self-storage facility collects sensitive personal information from our tenants in conjunction with the leasing process. The sensitive personal information may be used at our discretion to perform background checks, which may include a credit check, before the lease is executed, any time during the leasing process, and we may use this information in conjunction with collection of delinquent funds. The information may also be shared with law enforcement authorities.

Our files containing sensitive personal information are kept in a room accessible only by authorized representatives of this facility, or they are kept in a locked file cabinet, the key to which is only accessible by authorized representatives of this facility.

Our files containing sensitive personal information are disposed of either by shredding all document pages that contain sensitive personal information; erasing all sensitive personal information from documents, or otherwise modifying the document (such as blacking it out or burning it) to make the sensitive personal information unreadable or undecipherable.