IMPROVE YOUR FIRM'S DATA PRIVACY STRATEGY

Ten Tips for Better Data Privacy Implementation

The principles listed below can be used to guide the development of a robust privacy program. For more information, see the additional resources from the SIA Data Privacy Advisory Board listed at the bottom.

Use privacy impact assessments to identify deployments and applications that present higher risks to privacy.	Restrict access to data. Clearly define rules stating who has access and when and for what purpose access may be granted.
Minimize data collection by gathering only the necessary information for the intended purpose.	Embrace the concept of proportionality by offering stakeholders fair and explicit privacy options when they agree to use a product or service.
Store data for only as long as is reasonably necessary or required by law or regulation.	Support reciprocity by giving data subjects control over their privacy preferences as much as possible. Such privacy controls should be easy to use, and privacy should be the default, not an option.
Take reasonable steps to ensure that personal data is accurate. Offer data subjects the opportunity to correct errors.	Be transparent in presenting privacy options, practices and settings. Explain in plain language how and why personal data is being collected, used, shared, retained and disposed of.
Implement appropriate policies and procedures to process and store data in a secure manner.	Conduct regular reviews and audits to ensure compliance with legal and regulatory requirements and industry standards and best practices.

SIA DATA PRIVACY ADVISORY BOARD RESOURCES

The following resources are available on the SIA website, securityindustry.org.

– Reducing Risk, Seizing Opportunity: A Security Industry Guide to Privacy
– SIA Privacy Code of Conduct
– SIA Data Privacy Code of Practice – Video Surveillance

Security Industry Association
securityindustry.org
SIA