How Cos. Can Build Effective Data Privacy Appeals Processes

By **Steven Stransky** (March 17, 2021)

Steven Stransky

As state legislatures continue to introduce and debate data protection bills, businesses are constantly having to reassess whether they need to amend their compliance programs to account for new cybersecurity obligations or consumer data privacy rights, e.g., the right to access, correct or delete personal data.

Finding commonality among the states' disparate data protection requirements is key for businesses to streamline their compliance programs, and one requirement in particular — maintaining a formal data privacy rights appeals process — is gaining significant traction within various states. Accordingly, businesses should build a comprehensive appeals program that satisfies multiple state requirements.

However, there are a broad range of issues a business must address to ensure their data privacy rights appeals process is both practical and efficient.

The State Law Trend

As background, certain federal laws — e.g., the Freedom of Information Act and the Health Insurance Portability and Accountability Act — require federal agencies and certain private sector entities to implement appeals processes for when individuals exercise the data privacy rights afforded to them under the applicable law. State governments are requiring similar measures in the consumer context.

For instance, Virginia recently became the second state to enact a comprehensive consumer data protection law when it passed the Consumer Data Protection Act. The CDPA grants Virginia residents data privacy rights, imposes new obligations on certain types of businesses, known as controllers, that process their personal data and regulates how controllers must respond to consumers exercising their privacy rights.

The CDPA requires a controller to establish a process for a consumer to appeal the controller's refusal to take action with respect to a consumer's data privacy request and ensure the appeals process is conspicuously available and similar to the process for submitting the initial request.

Washington may be the next state to enact a consumer data protection law and its draft Privacy Act, S.B. 5062, has similar provisions as set forth in the CDPA. In particular, S.B. 5062 mandates that controllers establish an internal process whereby consumers may appeal a controller's refusal to take action with respect to a privacy request.

The appeal process, according to S.B. 5062, must be conspicuously available and as easy to use as the process for submitting the initial privacy request. S.B. 5062 sets forth the time frame in which appeals must be adjudicated, the manner in which appeals may be submitted, certain content that must be included in the controller's appeals decision, and record-retention obligations.

Some state legislatures, e.g., Connecticut and Utah, have introduced data protection bills that have data privacy appeals requirements similar to those in the CDPA and S.B. 5062. On

the other hand, some state data protection proposals, e.g., Alabama, Oklahoma and Illinois, only require businesses to respond to a consumer's privacy request with a description of any preexisting appeal rights the consumer may have, but do not impose any substantive obligations in this area.

As these bills move through the legislative process, organizations should monitor whether the notice of appeal clauses are amended to create more substantive requirements analogous to those in the CDPA and S.B. 5062.

Best Practices and Considerations

Like other compliance programs, businesses implementing data privacy request appeals processes should address their legal obligations in the context of their corporate structure and culture, available resources, and regulatory enforcement risk.

Although such compliance programs must be narrowly tailored to each organization, there are several best practices they can follow and considerations they should address to create an efficient and effective appeals program.

Initial Privacy Requests

An appeals program is only as strong as its initial data privacy request intake process. Standard data privacy intake procedures include documenting types of requests, time frames and responses.

In addition, it is particularly important for a business's privacy request intake record to clearly address whether the consumer's request was denied in full, or in part; the reasons for any denial; the databases and systems, if any, that were reviewed; and, all individuals who participated in the decision.

This record pertaining to an initial data privacy rights request will serve as the foundation for the entire appeals process and therefore must be detailed and comprehensive.

Structure

There are several structural issues a business must address when creating a data privacy rights appeals process, such as whether appeals will be adjudicated by one individual, e.g., the chief privacy officer or general counsel, or a multiperson board.

If a multiperson board is used, it must be determined how long individuals will serve on the board, whether it is their full- or part-time position, and whether labor laws restrict employees from serving in this capacity.

Given the short time frame in which appeals must be resolved, businesses should appoint secondary appeals adjudicators to be readily available in the event the primary adjudicator is not. Most importantly, appeals must be independent from the initial decision and insulated from internal or external pressure.

Standard of Review

The appeals process must clearly define its scope of review and apply it consistently. For instance, businesses need to decide whether the appellate adjudicators should only address whether the initial decision-making process adhered to internal protocols or be permitted to

engage in their own fact-finding to resolve data privacy requests.

Similarly, businesses need to decide whether appeals adjudicators can contact the consumer directly for more information or unilaterally change the underlying privacy request decision.

Notice

Businesses must provide clear and concise communications about their appeals processes that are often memorialized in website privacy statements. These notices must clearly address how the consumer can make an appeal, what information must or should be included in the appeal, how personal data submitted therein will be used and retained by the business, how the business may contact the consumer, applicable response time frames and the standard of review.

In addition to a privacy statement, a business may consider drafting other forms of communication, e.g., FAQs, to assist consumers wishing to exercise their rights to appeal.

Record-Keeping and Auditing

Businesses must properly document their privacy request and appeals protocols and delegations of authority and ensure they are easily accessible. They should keep metrics with respect to the volume of privacy requests and appeals adjudicated in a given time frame to anticipate future resource needs.

Also, the entire request and appeals program should undergo an independent audit to ensure that it is operating properly and efficiently.

Ultimately, an efficient and effective data privacy request appeals process can bring greater credibility to, and consumer confidence in, this fundamental aspect of data protection law. Having such a comprehensive process may also minimize the likelihood that consumers will file a complaint with a regulatory agency or that the company will be subject to a government investigation.

Steven G. Stransky is partner and vice chair of the privacy and cybersecurity practice group at Thompson Hine LLP.