Privacy & Data Security

Primary Contact

Eva Novick
Special Counsel, Team Leader
eva.novick@millernash.com
503.205.2472 | Portland Office

Companies collect, store, and process a wide range of personal information from customers and employees. Whether the data includes customer bank accounts, credit card information, or employee social security numbers, all businesses are custodians of sensitive data that are bound by privacy and security regulations.

Our attorneys advise clients on data security best practices, legal requirements, and industry-specific rules in an ever-changing landscape. In the event of a data breach, we work with companies to contain the breach, comply with notice requirements, and develop a strategic plan to prevent further issues.

Compliance

A patchwork of state and federal laws, and industry-specific rules, govern data security and the collection and use of data. We help our clients understand these regulations and draft information security policies to ensure compliance. We also help our clients make sure that they are providing proper notifications regarding how data is collected, stored, and used.

We advise on a broad range of compliance issues, including:

- Washington's My Health My Data Act (MHMD)
- California Consumer Privacy Act (CCPA)
- General Data Protection Regulation (GDPR)
- Telephone Consumer Protection Act (TCPA)
- Family Educational Rights and Privacy Act (FERPA)
- Website privacy policies—including drafting, reviewing, and/or revising policies to accurately disclose how websites are collecting, storing, and using data.

Data Breach

Our attorneys have assisted local and international companies, large and small, that have experienced a data breach. We help companies understand their legal obligations, investigate the source of the breach, develop a strategy for an appropriate response, and notify regulators and/or affected individuals. Our attorneys work with in-house counsel and IT departments in various industries on breach response.

Data Security Audits

Every company should establish and regularly update its policies on secure receipt, storage, and transmission of consumer and employee data. We help companies examine their practices, identify the data they are collecting, storing, and transmitting, and understand what the law or other rules require them to do regarding that data. With that information in hand, we help clients develop policies that are both compliant and compatible with their business goals. Once these policies are implemented, we provide continual updates to reflect new requirements and best practices.

Vendor Contracts, Risk Transfer & Insurance

Our attorneys understand the intersection of contractual law, insurance law, and data security. We have reviewed and negotiated hundreds of vendor contracts that involve these issues, including cloud computing, information technology, networking, data center, and database agreements in domestic and international transactions. We have extensive experience working with in-house legal departments, engineers, sales teams, and related departments.

Employee Training & Presentations

Keeping data secure and ensuring that data policies are properly executed requires awareness and understanding from all employees who handle that data. Our attorneys regularly give presentations and provide in-house training on the data security laws that pertain to a company and the best practices to avoid unauthorized persons from gaining access to data.