

# Privacy and Data Protection

All companies have privacy and data protection issues. A strong reputation for privacy and data security can bring positive attention to a business and help it win customer confidence in a crowded, competitive marketplace. Conversely, a single data breach can put millions of customer data, client documents or employee information in jeopardy causing businesses to lose billions of dollars each year. And the risks to businesses go beyond financial considerations—companies that fail to adequately safeguard confidential records can face legal liability and damaging publicity. Both courts and the public are taking an increasingly dim view of companies that fail to take reasonable efforts to protect sensitive employee and customer data.

The best approach is comprehensive planning and Womble Carlyle can help. We take a firm-wide, multi-practice approach to privacy and data protection, offering a variety of services to meet all of your needs in this rapidly evolving field, including:

- conducting privacy and security assessments;
- drafting and reviewing workplace policies and procedures;
- providing training to employees;
- managing privacy risks in contracts and mergers and acquisitions;
- keeping data safe when working with outside contractors and vendors; and,
- providing dedicated staffing for client privacy projects and ongoing privacy management.

Our team of attorneys has backgrounds in such wide-ranging fields as intellectual property litigation, technology and data security, regulatory compliance, health information confidentiality, telecommunications, labor and employment (particularly workplace privacy issues), and trade secrets.

Our focus is preventing data breaches before they occur. We will work with you to assess your privacy needs and develop a plan to alleviate all areas of vulnerability. We also can help you monitor and comply with any state or federal regulations affecting privacy and data protection issues.

Should the need arise, we effectively assist with data breaches and are experienced in representing our clients in litigation and in agency or law enforcement matters.

**For more information and a complete list of team members, please visit [www.wcsr.com/privacy](http://www.wcsr.com/privacy).**



**WOMBLE  
CARLYLE** <sup>®</sup>  
**INNOVATORS AT LAW**<sup>®</sup>

**[www.wcsr.com](http://www.wcsr.com)**

WOMBLE CARLYLE SANDRIDGE & RICE, PLLC 1008\_4998

GA | SC | NC | VA | DC | MD | DE |

©2008

**Who needs to manage compliance and risk regarding personally identifiable information and other sensitive information?**



WHO: 10 Examples	WHAT: Examples of privacy and data protection touch points	
Employers	<ul style="list-style-type: none"> <li>HIPAA Privacy Rule and Security Rule and related ERISA fiduciary duties for group health plans (medical, dental, vision, FSAs, EAPs)</li> <li>Fair and Accurate Credit Transactions Act/FTC Disposal Rule</li> <li>Acceptable use policies</li> </ul>	<ul style="list-style-type: none"> <li>Workplace monitoring and medical and drug screenings</li> <li>OSHA privacy provisions</li> <li>ADA privacy provisions</li> <li>Investigations and background checks (e.g., HP \$14.5 million fine, and new federal and California pre-texting laws)</li> </ul>
Owners and Custodians of Personal Data	<ul style="list-style-type: none"> <li>FTC Act § 5</li> <li>State unfair business practice laws</li> <li>Privacy notices and policies</li> <li>Security breach notice laws</li> <li><i>Bell v. Michigan Council</i>, 2005 Mich. App. LEXIS 353 (Mich. Ct. App. 2005) (court found duty to protect plaintiffs from identity theft and damages for “mental anguish” are permissible)</li> </ul>	<ul style="list-style-type: none"> <li><i>Guin v. Brazos Higher Education Foundation Service</i>, Civ. No. 05-668, 2006 U.S. Dis. Lexis 4846 (D. Minn. 2006) (employer not liable for data theft by employee because it had implemented proper controls)</li> <li>SSN protection (e.g., NCGS §75-62)</li> <li>Outsourcing data controls</li> <li>UETA and E-SIGN</li> </ul>
Owners and Custodians of Trade Secrets	<ul style="list-style-type: none"> <li>Data protection as an element of trade secrets claim</li> </ul>	<ul style="list-style-type: none"> <li>Non-disclosure agreements</li> <li>Vendor due diligence</li> </ul>
Sales and Marketing Managers	<ul style="list-style-type: none"> <li>CAN-SPAM</li> <li>Do-Not-Call</li> <li>FTC Telemarketing Sales Rule</li> <li>FTC Fax Ban Rule</li> </ul>	<ul style="list-style-type: none"> <li>Behavioral targeting and company data governance policies</li> <li>State telemarketing and fax rules</li> <li>Children’s Online Privacy Protection Act</li> </ul>
International Companies	<ul style="list-style-type: none"> <li>Off-shoring data controls</li> <li>Comprehensive privacy protection laws in Europe, Australia, etc.</li> <li>Cross-border transfers of employee and customer data</li> </ul>	<ul style="list-style-type: none"> <li>Highly regulated use of personal information (e.g., Spanish law firm fined for sending marketing message to individual who had provided business card)</li> </ul>
Corporations, Public Companies, and other SEC-Regulated Entities	<ul style="list-style-type: none"> <li><i>In Re Caremark International Inc. Derivative Litigation</i>, 698 A.2d 959 (Del. Ch. 1996) (duty of care applied to oversight of information systems)</li> <li>Form 10-K filings (Government Regulation and Risk Factors sections)</li> <li>Private Placement Memoranda</li> <li>SEC Rule 30 (broker/dealer safeguards and disposal rules)</li> <li>SOX § 404 (integrity controls for financial data)</li> </ul>	<ul style="list-style-type: none"> <li><i>Goldberg v. ChoicePoint, Inc.</i> (No. BC329115 Cal. Sup. Ct., Los Angeles, filed February 18, 2005) (consumer class action regarding data breach); <i>Perry v. ChoicePoint, Inc.</i> (No. CV-05-1644 C.D. Cal, filed March 4, 2005) (shareholder derivative suit)</li> <li>Mergers and acquisitions (privacy due diligence and risk allocation)</li> <li>Privacy of shareholder personal information</li> </ul>
Regulated Industries (Financial services, insurance, health, energy, public utilities, government, higher education, etc.)	<ul style="list-style-type: none"> <li>HIPAA Privacy Rule and Security Rule</li> <li>Gramm-Leach-Bliley Act (Board oversight required)</li> <li>FTC Privacy Rule and Safeguards Rule</li> <li>State insurance, financial, health privacy laws</li> <li>Federal Financial Institutions Examination Council Risk Assessment and Authentication Guidelines</li> </ul>	<ul style="list-style-type: none"> <li>Self-regulation standards (e.g., North American Electric Reliability Corporation (NERC) Critical Information Protection guidelines)</li> <li>Family Educational Rights and Privacy Act (student privacy)</li> </ul>
Technology Companies	<ul style="list-style-type: none"> <li>Spyware (Sony/BMG \$4.25 million settlement)</li> </ul>	<ul style="list-style-type: none"> <li>“Privacy by design” in product development</li> </ul>
Payment Card Merchants, Banks, and Processors	<ul style="list-style-type: none"> <li>Payment Card Industry Data Security Standards 1.1</li> </ul>	<ul style="list-style-type: none"> <li>PCI Data Security vendor contracts and due diligence</li> </ul>
Litigants	<ul style="list-style-type: none"> <li>Protective order obligations</li> <li>Filing personal data in court records (e.g., NCGS §75-65 prohibition and penalties)</li> <li>Discovery/Subpoenas</li> <li>Federal Rules of Civil Procedure eDiscovery requirements</li> </ul>	<ul style="list-style-type: none"> <li><i>American Express v. Vinhnee</i>, 336 B.R. 437; 2005 Bankr. LEXIS 2602 (9th Cir. B.A.P. 2005) (electronic records inadmissible due to inadequate showing of authenticity based on data security controls)</li> </ul>

[www.wcsr.com/privacy](http://www.wcsr.com/privacy)

GEORGIA SOUTH CAROLINA NORTH CAROLINA VIRGINIA WASHINGTON, DC MARYLAND DELAWARE

©2008 Womble Carlyle Sandridge & Rice, PLLC 0908\_4631