OUR PRACTICE

GDPR

Baker Donelson's General Data Protection Regulation (GDPR) team consists of data protection, privacy, and cybersecurity attorneys who assist our diverse client base, which ranges from entrepreneurs to non-profits to Fortune 500 companies, with GDPR matters spanning a wide variety of industries. Our experienced GDPR team guides clients through every phrase of the compliance process, from compliance program creation and gap analysis, to ongoing assistance with documentation and decision-making, according to a pace and level of engagement driven by each client's unique priorities and resources.

Our GDPR team closely monitors the rapidly evolving regulatory landscape, including European Union (EU) member state laws, guidelines and opinions, sectoral requirements, and best practices. Our team members are active participants in the privacy community and demonstrated GDPR subject matter expertise through regular client engagement, frequently serving as authors and speakers on GDPR-related topics, earning accreditations from the world's largest information privacy organization, the International Association of Privacy Professionals (IAPP), including Certified Information Privacy Professional (CIPP) in the United States (CIPP/US), Canada (CIPP/C) and Europe (CIPP/E), and Certified Information Privacy Manager (CIPM) certifications, and lending leadership and support to the IAPP's Nashville chapter of KnowledgeNet.

Our GDPR team also regularly partners with leading GDPR compliance consultants and vendors who build on our legal advice by providing our clients with comprehensive and international research services, EU-based legal support (through our TerraLex global network membership), onsite and offsite technology consultants, and EU representative and data protection officer services.

In the years leading up to and since the GDPR went into effect on May 25, 2018, our GDPR team has consistently been retained to advise clients facing compliance with this new and complex area of international privacy law and demonstrated its expertise with advising clients on the applicability of the GDPR to online and offline activities, as well as navigating the myriad of legal, operational, technological, and business-related aspects of compliance.

This comprehensive privacy regulation, which governs the processing of personal data of individuals in the European Union and European Economic Area, has captured the attention of many of our clients, especially with respect to its extraterritorial enforcement in non-EU countries such as the United States and Canada and tiered system of harsh fines which can amount to the greater of four percent of annual global revenue or 20 million euros.

Our GDPR team is also skilled at responding to our clients' requests for guidance as to how the requirements of the GDPR compares with those of other privacy regulations and security standards on which we regularly advise, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the California Consumer Privacy Act of 2018 (CCPA), National Institute of Standards and Technology (NIST) Computer Security Standards, the Canadian Personal Information Protection and Electronic Documents Act, and related Federal Trade Commission rules, among others.

How Do You Know if the GDPR Applies to Your Company?

Organizations (for profit and non-profit) that process personal data of natural persons ("data subjects") will be subject to the GDPR if they:

- ***have a business presence (physical or otherwise) in the EU/EEA*** and the processing activities relate to the business activities in the EU/EEA (even if the processing takes place elsewhere); or
- ***do not have a business presence in the EU/EEA*** and the data processing activities relate to the offering of goods or services to, or the monitoring of data subjects located in the EU/EEA.

Under the regulation, the definitions of which business activities constitute "processing," what is required to establish a business presence in the EU/EEA, and the types of offline and online data that may constitute "personal data" can be quite broad.

How Can We Help You?

Our team helps clients address the multitude of issues raised by GDPR compliance, including, but not limited to:

- Gap analysis, risk assessment, audit support, and remediation for day-to-day operations and merger and acquisition events
- Identification and categorization of data and data flows to meet data mapping and documentation requirements
- Drafting and negotiating Data Protection and Data Sharing Agreements for the enterprise and between independent entities
- Identifying cross-border data transfer strategies, including standard contractual clauses, Binding Corporate Rules, and reliance on adequacy decisions
- Vendor / third-party service provider management and diligence
- Preparing self-assessments, questionnaires, templates, and playbooks
- Customized C-Suite, employee, and subcontractor training using various approaches (lecture, webinar, interactive, and train-the-trainer)
- Advice on addressing data subject access requests and rights
- Privacy policies (addressing cookies and analytics), notices, and terms for websites and mobile applications
- Social media and website risk assessments
- Contract negotiation
- Responding to supervisory authorities and evaluating local requirements
- Requirements for engaging EU representatives and Data Protection Officers
- Internal policies and procedures
- Drafting and advising on information security program and policies
- Incident response and data breach strategies and support
- Cross-Border Discovery, disclosure, and internal investigations

Representative Matters

- Advise clients on developing GDPR compliance policies and procedures, including data retention and destruction, data incident and breach response, employee privacy and data subject access requests, website privacy policies and terms of use, among others.
- Advise domestic and international businesses regarding cross-border transfer mechanisms, including standard contractual clauses and Privacy Shield compliance and certification.
- Conduct Privacy Risk Assessments (PIAs/DPIAs) for new programs, systems, processes, and high risk activities.
- Update online and offline data privacy policies in line with applicable laws, with special attention to regarding disclosure to third parties, advertising, and processing through cookies and other similar technologies, (including website and mobile applications).
- Review mobile applications and similar products for compliance with GDPR and third-party terms of use (Twitter, Amazon, Yahoo, etc.).

- Advise on breach notification protocol to affected individuals and process on reporting to regulators, credit agencies, and law enforcement.
- Advise on data privacy requirements for third parties (e.g., clients, vendors, processors, affiliates) and incorporate data privacy into operational training (e.g., HR, marketing, call center).
- Conduct due diligence around the data privacy and security posture of potential vendors and processors.
- Draft and negotiate data processing agreements and addenda for controller, processor, and subprocessor roles, third party data sharing agreements, and intercompany data sharing agreements.
- Assess website and mobile application functionality and advise on required and optional customer-facing privacy notices and terms of use for compliance with GDPR and other data protection regimes.
- Analyze use cases for compliance with lawful processing requirements, data mapping, privacy assessments, and documentation of same.
- Counseled a video and chat service on compliance for its mobile application and management of its data subject access requests.
- Advised a leading consumer products company on all aspects of GDPR compliance for a portfolio of brands sold in the U.S., Canada, and the EU/EEA with an emphasis on website compliance.
- Advised manufacturers regarding the applicability of GDPR due to having distributors in EU countries.
- Advised an online publisher on applicability of GDPR as well as assisted with Privacy Shield registration and assisted in preparation of GDPR Legitimate Interest Assessments related to certain data processing activities, and prepared example GDPR consent language for online forms.
- Advised a global supplier of industrial materials on communicating GDPR compliance internally and to customers. Also provided compliance advice relating to website privacy notice and terms of use.
- Assisted investment management firm with updates to Investment Advisory Agreement and privacy statement.
- Advised software companies on updating their website privacy notices and terms of use for company websites and apps.
- Monitor and advise on international data privacy and data protection developments.