CLARK HILL

General Data Protection Regulation

Effective May 25, 2018

General Data Protection Regulation
Effective May 25, 2018

The European Union's ("EU") General Data Protection Regulation ("GDPR") is fast approaching, and it is far-reaching, as it will affect a significant number of organizations across the globe, even if they are not located in the EU. We provide key information to help impacted organizations understand their obligations under the GDPR and prepare for GDPR compliance.

What is the GDPR?

The GDPR is the EU's new regulatory framework governing the collection, use, storage, and destruction of personal data of EU residents. While the full scope and reach of GDPR are yet to be tested, the GDPR's intended scope includes organizations located outside the EU that process personal data of EU residents relating to marketing goods or services to EU residents, or monitoring the behavior of EU residents as their behavior takes place within the EU.

Data protection is a fundamental right for EU citizens. The current data protection framework is based on the Data Protection Directive 95/46/EC that was adopted in 1995. Since then, there have been significant advances in information technology and fundamental changes to the ways in which individuals and organizations communicate and share information. In addition, the various EU Member States have taken different approaches to implementing the Data Protection Directive, which created compliance difficulties for organizations conducting business in more than one EU Member State. To address the realities of globalization of information on the one hand, and fragmentation of implementation of existing data protection laws on the other hand, the EU's legislative bodies prepared an updated and more harmonized data protection legislation, backed by strong enforcement, to protect an individual's personal data and the free movement of such data, which is known as the GDPR.

The GDPR sets forth various new measures with which organizations must comply to protect EU residents' fundamental rights and freedoms relating to the processing of their personal data, and the free movement of personal data.[1]

Compliance is required by May 25, 2018. The risks of non-compliance include fines of up to 4 percent of global annual revenues or 20 million euros, whichever is greater. Under the GDPR, designated authorities have increased enforcement powers to impose fines on organizations that do not comply with GDPR.

Does GDPR Apply to You?

The GDPR applies to any organization that is a processor or controller of EU residents' personal data, including both for-profit and nonprofit organizations. The GDPR defines a controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[2] In essence, the controller is the entity that makes decisions about processing activities, regardless of whether it actually carries out any processing operations. The processor is any person or entity which carries out the processing on behalf of the

[1] Recitals 1, 2, and 3 of the GDPR. For purposes of this informational brochure, all references to text provisions such as Recitals and Articles shall pertain to the GDPR.
[2] Article 4(7).

controller.[3] The GDPR applies to organizations of all sizes that process personal data of EU residents or monitor the behavior of EU residents in the EU, although small and medium sized businesses may be exempt from record-keeping requirements under limited circumstances.

The GDPR provides that the regulations apply to organizations located in the EU that process personal data, regardless of whether the processing takes place in the EU or not; and also apply to organizations located outside the EU that process personal data of data subjects who are in the EU where the processing activities are related to: "(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."[4]

"Personal data" refers to any information of an individual who is or can be identified, directly or indirectly, either from the data or from the data in conjunction with other information that is or likely to come into the possession of the data controller.[5] Accordingly, any information relating to an identified or identifiable natural person may fall under the umbrella of personal data. The GDPR identifies "special categories of personal data" that relate to a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; the physical or mental health or sex life and sexual orientation of the data subject; and genetic data and biometric data for purposes of identifying an individual.[6] Organizations are prohibited from processing these special categories of personal data, except under specific limited circumstances.[7]

If your organization obtains personal data from EU residents, including EU resident employees and customers, in the course of providing goods and services, the GDPR will apply to the collection, processing, use, and storage of such personal data.

In addition, to the extent that organizations may employ other companies to process such personal data on their behalf, such organizations must address GDPR compliance with respect to their vendors. Both data controllers and data processors are subject to the GDPR.

Top 10 Operational Impacts and for GDPR Compliance

The GDPR introduces several new concepts and approaches, and the legislation is comprehensive and complex. It will be important for organizations to review their data protection compliance programs and prioritize their initiatives for GDPR preparedness as they approach the upcoming deadline**.** We provide a list of the top 10 operational impacts and best practice considerations for GDPR compliance.

****The top 10 list is for general informational purposes and nothing herein constitutes legal advice by Clark Hill PLC to any organization. Each organization should consult with its legal counsel and/or the appropriate privacy professional for a customized assessment of its specific risks and needs for GDPR compliance.*

[3] Article 4(8).
[4] Article 3.
[5] Article 4(1).
[6] Article 9.
[7] Article 9(2) lists those circumstances where the prohibition of processing special categories of personal data do not apply.

1. Mandatory Privacy by Design and Privacy Impact Assessments

Under the GDPR, data controllers bear the responsibility for assessing the degree of risk that their processing activities pose to data subjects and in implementing controls that map to the risk. In that regard, one of a data controller's significant responsibilities include the duty to implement data protection by design and perform mandatory privacy impact assessments as appropriate. The GDPR requires that controllers utilize appropriate technical and organizational measures which are designed to implement data protection principles, and this implementation is required to be considered at the time of determining the means for processing and at the time of the processing itself.[8] Controllers should design products with privacy in mind rather than addressing it after an incident occurs that poses a potential or actual personal data breach. Controllers are also required to "implement technical and organizational measures to ensure that, by default, only personal data which are necessary for each specified purpose of the processing are processed."[9] Accordingly, privacy protective settings should be the default in any product.[10]

Where processing is likely to result in a high risk for the rights and freedoms of EU residents, controllers must first carry out a data protection impact assessment and consult with the lead supervisory authority before processing takes place.[11] A data protection impact assessment is required in certain cases involving systematic and extensive automated processing or processing on a large scale of special categories of personal data, as well as those cases where a supervisory authority deems to warrant such an assessment.[12] The GDPR identifies the required components of the assessment, and factors to consider as part of the assessment.[13]

2. Cybersecurity Standards

The GDPR imposes strict security standards on data processors and data controllers relating to the processing of personal data, and delineates the separate duties and responsibilities of data controllers and data processors towards meeting these security standards. Data controllers are obligated to engage only those processors that provide "sufficient guarantees to implement appropriate technical and organizational measures" to meet the GDPR's requirements and protect data subjects' rights.[14] Processors must also take various measures to implement the GDPR's "security of processing" standards.

Data controllers and processors must "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" while "taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing" as well as the risk of likelihood and severity of impact to the rights and freedoms of individuals.[15] The GDPR identifies those factors which may constitute security measures "appropriate to the risk" to include the following:

---

[8] Article 25(1).
[9] Article 25(2).
[10] Article 25(2).
[11] Articles 35, 36. The "Supervisory Authority" is the public authority appointed in each Member State to monitor application of the GDPR. See Article 51.
[12] Article 35.
[13] Article 35.
[14] Article 28.
[15] Article 32.

- The "pseudonymisation"[16] and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the personal data in a timely manner in the event of an incident;
- A process for regularly testing, assessing and evaluating the effectiveness of the organization's security measures.[17]

The GDPR encourages the creation of approved codes of conduct and certification mechanisms to govern the application of GDPR provisions and ensure that appropriate safeguards are met.[18] Data controllers and processors that adhere to an approved code of conduct or an approved certification mechanism may use these tools as a factor to help demonstrate compliance with the GDPR's security standards.[19]

3. Individual Consent

Consent remains the lawful basis for obtaining and processing personal data under the GDPR, but individual consent may be harder to obtain. Given the tightening of consent rules under the GDPR, this will be one of the leading operational impacts for many organizations under the GDPR.

Conditions of Consent: The GDPR places conditions for consent and requires that the controller be able to demonstrate that the data subject consented to processing of his or her personal data.[20] The GDPR requires the data subject to demonstrate consent by a "statement or a clear affirmative action" establishing that the consent was "freely given, specific, informed and unambiguous".[21] Under Recital 32 of the GDPR, the consent may include ticking a box on an internet website, choosing technical settings for "information society services," or another statement/conduct which clearly indicates the data subject's agreement for the proposed processing of his or her personal data. Where data controllers previously may have relied on implicit and "opt-out" consent, the GDPR specifically does not allow "silence, pre-ticked boxes or inactivity" to confer consent.[22]

In the course of obtaining the data subject's statement or a clear affirmative action, the GDPR requires that the consent must be specific to each data processing operation. A request for consent to data processing must be "clearly distinguishable" from any other matters, and it must be provided "in an intelligible and easily accessible form, using clear and plain language."[23] The Regulations exempt controllers from obtaining consent for subsequent processing operations if the operations are

[16] Article 4(5). "Pseudonymisation" is a new concept in European data protection law that provides a mechanism for rendering data to be neither anonymous nor directly identifying. Pseudonymisation means the processing of personal data in a manner that the personal data can no longer be attributed to a specific data subject without using additional information that is held separately and subject to safeguards to ensure that the personal data are not attributed to an identified or identifiable natural person. Article 4(5).
[17] Article 32.
[18] Articles 40, 42.
[19] Article 32.
[20] Article 7.
[21] Recital 32 provides: "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."
[22] Recital 32.
[23] Article 7.

"compatible", but there is no bright line rule for what constitutes compatibility, as it would be determined by reviewing various fact-specific factors including the link between the processing purposes, the context within which the personal data was collected, the reasonable expectations of the data subject, relationship between the controller and data subject, etc.[24]

There is a presumption that consent is not freely given under the circumstances where there is a "clear imbalance between the data subject and the controller, in particular where the controller is a public authority" and it is unlikely that consent was freely given under the circumstances.[25] Significantly, a controller may not make a service conditional upon consent, unless the processing is necessary for the service.[26]

Organizations that obtain personal data which are particularly sensitive in nature such as health information and biographical information and therefore, "deserve specific protection", the GDPR requires a higher level of consent – explicit consent - for the processing of these "special categories of personal data".[27] Accordingly, a user's conduct or choice of browser settings, which may constitute appropriate consent for personal data, will likely be inadequate to meet the explicit consent requirement for special categories of personal data. Further, the GDPR allows Member States to enact laws that restrict the processing of some categories of data even if the data subject explicitly consents.[28]

Individual Right to Withdraw Consent/Right to Erasure: Importantly, the GDPR gives data subjects the right to withdraw consent at any time and "it shall be as easy to withdraw consent as to give it."[29] The GDPR requires that controllers inform data subjects of their right to withdraw consent before it is given. Once consent is withdrawn, data subjects have the right to have their personal data erased "without undue delay" and no longer used for processing under certain circumstances.[30] The data subjects also have a right to obtain a copy of their personal data and restrict its use.[31]

Parental Consent for Children's Personal Data: The GDPR also requires parental consent for processing children's personal data under the age of 16, but allows Member States to set a lower age of consent not below 13 years.[32] Unless otherwise provided by a Member State, a controller must obtain the consent of a parent or guardian when processing the personal data of a child under the age of 16. Controllers are required to make "reasonable efforts" to verify that consent was obtained by the holder of parental responsibility over the child, "taking into consideration available technology."[33]

4. Strict Data Breach Notification Rules

The GDPR provides strict data breach notification rules.[34] The GDPR defines a "personal data breach" as being a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.[35] In

[24] Article 7; Recital 50.
[25] Recital 43.
[26] Recital 43.
[27] Article 9.
[28] Article 9.
[29] Article 7(3).
[30] Article 17.
[31] Article 18.
[32] Article 8.
[33] Article 8.
[34] Articles 33, 34, Recitals 85, 86.
[35] Article 4(12).

the case of a personal data breach, GDPR requires the data controller to notify the appropriate supervisory authority of all data breaches without undue delay and where feasible not later than 72 hours after having become aware of it, unless the data breach is unlikely to result in a risk for the rights and freedoms of the individuals.[36] Proper notification to the affected data subject must be given "without undue delay".[37]

Notification to the authority and to the affected data subject must include certain types of information as set forth in detail in the GDPR. The GDPR also provides exceptions to the requirement to notify data subjects under certain circumstances such as if the data was encrypted and unintelligible to an unauthorized user, or that a high risk for the rights and freedoms of data subjects is unlikely to materialize, or when notification to each affected data subject would involve "disproportionate effort" in which case a data controller may use alternative communication measures.[38]

In addition, the controller must comply with documentation requirements to record any data breaches including the facts relating to the personal data breach, its effects and the remedial action taken.[39] This documentation is intended to enable the supervisory authority to verify the controller's compliance.

To help comply with the GDPR's breach notification rules, an organization should have in place the appropriate policy and procedure to ensure that any detected breach of personal data is not only timely reported to the appropriate supervisory authority and affected data subjects, but also a process for identifying the individual(s) who will be responsible for performing the investigation of a personal data breach and proper recordation of the incident and the organization's corrective action taken.

5. Vendor Management

Data controllers have specific responsibility for complying with the GDPR's provisions. Controllers are liable for the actions of the processors they select and are responsible for compliance with the GDPR's personal data processing principles. When selecting a processor, controllers must use processors that provide sufficient guarantees of their abilities to implement the technical and organizational measures necessary to meet the GDPR requirements.[40] Accordingly, it is critical that the controller take measures to ensure that the processors they select equally comply with the GDPR requirements.

Carefully selecting the appropriate processor will be particularly important if the personal data involves sensitive information that fall under the special categories of personal data, such as health information, biographical information concerning ethnic origin and philosophical beliefs of families, which are information that may be obtained in the course of an organization's activities. The controller may consider carrying out a data protection impact assessment prior to selecting a processor.

Importantly, once selected, the controller is required to have an appropriate service contract in place to govern the relationship between the controller and processor to ensure that the processor handles the personal data in compliance with GDPR.[41] Appropriate contractual provisions must include

[36] Article 33.
[37] Article 34.
[38] Article 34.
[39] Article 33.
[40] Article 28.
[41] Article 28.

the "subject-matter and duration of the processing" (i.e., the details of the processing and how and when data will be returned or deleted after processing), the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.[42] The GDPR lists specific obligations of the processor which must be included in the contract.[43]

6. Appointing a Data Protection Officer

Where appropriate, organizations must evaluate a requirement for a Data Protection Officer (DPO) if they process and store large amounts of EU residents' personal data. Generally, the DPO is tasked with ensuring the organization's compliance with the GDPR and must be involved in all issues of the controller and processor which relate to the protection of personal data,[44] advise the controller or processor of their obligations under applicable data protection laws, monitor compliance, and serve as the contact point for communications with the supervisory authority on issues relating to data processing.[45] A qualified DPO is based on his or her "professional qualities", should possess expert knowledge of data protection laws and practices, and be able to fulfill the enumerated tasks of a DPO.[46] The DPO may be appointed from the organization's staff or may fill the position as an independent contractor.[47] Data controllers and processors must appoint a DPO in any case where the processing is carried out by a public authority except for judicial courts; or the core activities consist of processing operations that involve regular and systematic monitoring of data subjects on a large scale; or the core activities consist of processing on a large scale of special categories of personal data and personal data relating to criminal convictions and offenses.[48]

In all other cases, a DPO is not mandatory. However, the controller or processor may designate a DPO to represent their interests with respect to their data protection programs. A group of enterprises may also appoint a single DPO as long as that DPO is easily accessible from each establishment.[49]

7. Individual Right to Data Portability

Where personal data is processed through automated means, data subjects have a new right to obtain their personal data from the data controller in a structured, commonly used and machine-readable format and the right to transmit that data to another controller.[50] Data subjects also have the right to have the personal data transmitted directly from one controller to another, if technically feasible. This right of data portability aims to provide more control and added choices to data subjects on how their data will be used and by whom.

The right to data portability applies to personal data that was originally processed based on the data subject's consent or by contract, and does not apply to processing that was necessary to carry out a public interest or processed by an official authority vested in the controller.[51]

---

[42] Article 28(3).
[43] Article 28(3).
[44] Article 38.
[45] Article 39.
[46] Articles 38, 39.
[47] Article 37
[48] Article 37.
[49] Article 37.
[50] Article 20.
[51] Article 20.

8. Profiling

In certain circumstances, individuals will have the right to object to their personal data being processed in a manner which includes profiling. "Profiling" is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."[52]

The GDPR places restrictions on a data controller's ability to perform automated processing of personal data, as well as to make decisions based on profiling.[53] Further, data controllers are required to provide the data subject with any information necessary "to ensure fair and transparent processing".[54] This includes notifying the data subject of the existence of profiling, the consequences of such profiling, and the data subject's right to object to profiling.

Data subjects have the right to object at any time to the automated processing of their personal data, even if done for lawful purposes under the GDPR such as the public interest. Data subjects also have the right to object to profiling relating to direct marketing.[55] Once the data subject objects, the personal data must no longer be processed for such purposes, with certain exceptions.[56]

9. Data Subject Access Requests

A data subject has the right of access to personal data which have been collected concerning that individual, and to exercise that right easily and at reasonable intervals.[57] Organizations must reply within one month from the date of receipt of a data subject's request to access personal information, and provide more information than was required under the previous Data Protection Directive.

10. Cross-Border Data Transfers

The GDPR permits the transfer of personal data to third countries or international organizations, as long as certain conditions are met. First, the data controller and processor must comply with the data protection security standards and measures set forth in the GDPR. Second, the controller and processor must obtain the European Commission's decision that the transferee country or international organization maintains an adequate level of protection, by evaluating a myriad of factors set forth in the GDPR.[58] This is referred to as an "adequacy decision".[59]

In the absence of an adequacy decision, a data controller or processor may transfer personal data to a third country or an international organization, if the controller or processor has provided "appropriate safeguards, and on condition that enforceable data subject rights and effective remedies for data subjects are available."[60] Appropriate safeguards which do not require any specific authorization from a supervisory authority may include a legally binding and enforceable instrument between public

[52] Article 4(4).
[53] Articles 21, 22.
[54] Recital 60.
[55] Article 21.
[56] Article 21(1).
[57] Recital 63, Article 18.
[58] Article 45.
[59] Article 45.
[60] Article 46.

authorities; binding corporate rules; standard data protection clauses approved or adopted by the European Commission; or an approved code of conduct or approved certification mechanism together with binding and enforceable commitments by the controller or processor in the third country to apply the appropriate safeguards relating to data subjects' rights. Personal data transfers to a third country or international organization is permissible via privately negotiated contractual clauses between the transferor and transferee controller and/or processor to apply appropriate safeguards, but this arrangement must be authorized by the appropriate supervisory authority.[61]

The United States has not achieved an adequacy determination by the EU Commission. To bridge the gap, and to continue fluid information transfer between the EU and U.S., the U.S. adopted the Safe Harbor framework in 2000, supplanted by the Privacy Shield in 2016. By adopting the Privacy Shield, entities in the U.S. currently can satisfy the compliance requirements and become in effect safe "islands" to which the EU then allows information to be transferred.[62] Notwithstanding its adequacy determination, relevant stakeholders in the EU continue to debate the future role of Privacy Shield once the GDPR comes into full force.

The GDPR provides additional specific circumstances and exceptions where personal data transfers to a third country or international organization may be permitted such as where the data subject has explicitly consented after being informed of the possible risks due to the absence of an adequacy decision and appropriate safeguards, the transfer is necessary for important reasons of public interest, or the transfer is necessary to protect the vital interests of the data subject where the data subject is incapable of giving consent, among other situations.[63]

What Should I Do Next?

- **Know Your Data.** Sounds obvious but the place to begin is with a comprehensive data audit identifying, among other items, sources of data, specific categories of data collected, who is it collected from and how, how is it stored, how is it used, how long is it kept. Identification of this information will help evaluate those areas that the organization will need to address and strengthen in order to comply with the GDPR. Organizations should engage knowledgeable professionals to help conduct an audit to identify the organization's information workflow and conduct a GDPR compliance analysis.

- **Know Your Policies and Procedures.** Organizations should adopt appropriate practices to deal with GDPR's requirements including practices on breach response, notification and documentation; obtaining appropriate consent; how to timely address instances where the data subject withdraws consent, exercises his or her right to have personal data erased or objects to profiling, and makes a subject access request; and documentation of compliance activities. Organizations should update their existing policies to reflect those practices.

[61] Article 46.
[62] Article 45. The Privacy Shield received an adequacy determination on July 12, 2016. In its first annual review, the EU Commission determined that the Privacy Shield continued to ensure an adequate level of Protection. "Report from the Commission to the European Parliament and The Council" (10/18/17). However, the Privacy Shield continues to operate in a climate of uncertainty and many stakeholders challenge whether it should be deemed adequate. See "EU – U.S. Privacy Shield – First annual Joint Review" (Article 29 Data Protection Working Party, November 28, 2017).
[63] Articles 48, 49.

- **Engage C Suite**. The potential fines and penalties for non-compliance are one of the most notable features of the GDPR. Make sure top level executive and board members are aware of, and engaged in, the process and ensuring budgets are in place to support any changes.

- **Prepare a Compliance Plan.** This should reflect the results of your data, policy and procedure, and compliance assessments. Identify concrete actions/steps, who is responsible, and when the item needs to be completed.

- **Review Your Vendor Contracts**. The GDPR requires vendors and service providers that process data regulated under the GDPR to be likewise compliant. Organizations should review their vendor contracts to include mandatory GDPR compliant provisions with their existing and future vendors.

- **Update Your Privacy Policy.** The changes over existing standards make it very likely that you will need to update your privacy policy to ensure they reflect your practices in compliance with applicable GDPR requirements. Important areas to note will include documentation of a lawful purpose for the collection and processing of data you collect; and properly notify data subjects of their rights under the GDPR such as clear procedures for seeking and revoking consent, the "right to erasure/right to be forgotten", and subject access requests.

- **Train and Communicate To Employees**. Develop and implement ongoing training to employees concerning the organization's data protection measures and their role in the process.

- **Continue Regular Reviews of Data, Security and Compliance Issues.** Not only is this essential for cybersecurity purposes but also for monitoring compliance with GDPR requirements in the face of an organization's changing circumstances.

- **Consider Cybersecurity Insurance**. Organizations should consider obtaining cybersecurity insurance which may help them manage certain financial exposures arising out of a data security breach or a cyber event.

CLARK HILL

CONTACT:

John L. Hines, Jr.
312.985.5927
hines@clarkhill.com

Sue S. Junn
213.417.5188
sjunn@clarkhill.com

OFFICES:

Birmingham
151 S. Old Woodward, Suite 200, Birmingham, MI 48009
P: 248.642.9692 | F: 248.642.2174

Chicago
130 E. Randolph St., Suite 3900, Chicago, IL 60601
P: 312.985.5900 | F: 312.985.5999

Detroit
500 Woodward Ave, Suite 3500, Detroit, MI 48226
P: 313.965.8300 | F: 313.965.8252

Dublin, Ireland
Fitzwilliam Hall**,** Fitzwilliam Place, Dublin, D02 T292
P: +353 (0)1 9011 115 | F: +353 (0)1 6694 798

Grand Rapids
200 Ottawa NW, Suite 500, Grand Rapids, MI 49503
P: 616.608.1100 | F: 616.608.1199

Lansing
212 East Grand River Ave, Lansing, MI 48906
P: 517.318.3100 | F: 517.318.3099

Las Vegas
3800 Howard Hughes Parkway**,** Suite 500**,** Las Vegas, NV 89169
P: 702.862.8300 | F: 702.862.8400

Los Angeles
1055 West Seventh Street**,** Suite 2400, Los Angeles, CA 90017
P: 213.891.9100 | F: 213.488.1178

Morgantown
1290 Suncrest Towne Centre, Morgantown, WV 26505
P: 304.233.5599 | F: 304.907.2130

Philadelphia
One Commerce Square, 2005 Market St, Suite 1000, Philadelphia, PA 19103
P: 215.640.8500 | F: 215.640.8501

Phoenix
14850 N. Scottsdale Rd, Suite 500, Scottsdale, AZ 85254
P: 480.684.1100 | F: 480.684.1199

Pittsburgh
One Oxford Centre, 301 Grant St, 14th Floor, Pittsburgh, PA 15219
P: 412.394.7711 | F: 412.394.2555

Princeton
210 Carnegie Center, Suite 102, Princeton, NJ 08540
P: 609.785.2968 | F: 609.785.2999

San Diego
One America Plaza, 600 West Broadway, Suite 500, San Diego, CA 92101
P: 619.557.0404 | F: 619.557.0460

San Francisco
One Embarcadero Center, Suite 400, San Francisco, CA 94111
P: 415.984.8500 | F: 415.984.8599

Washington D.C.
1001 Pennsylvania Ave NW, Suite 1300 South, Washington, D.C. 20004
P: 202.772.0909 | F: 202.772.0919

Wilmington
824 N. Market St, Suite 710, Wilmington, DE 19801
P: 302.250.4750 | F: 302.421.9439