A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

First Edition

MERITAS®
LAW FIRMS WORLDWIDE

A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

Dennis Unkovic, Editor

du@muslaw.com
Tel: +1-412-456-2833

Meyer, Unkovic & Scott LLP
www.muslaw.com

Not so long ago, "data protection" meant a locked filing cabinet and a good shredder. No longer. In a single generation, protecting data went from safeguarding documents to securing information of almost every kind, both tangible and in electronic form. Although everyone understands what it means to protect a hard copy document, it is much harder to conceptualize protecting intangible information. To make matters worse, a data breach today can cause far more serious consequences than in years past. To cite just one example, the improper disclosure of one's personal data can easily result in identity theft, with the victim often left unaware of the crime until it is far too late to stop it.

With the endless march of technology and an increasingly connected world, protecting personal data is clearly more important than ever. In response, governments around the world have focused on enacting legislation to keep up with the fast pace of change. The EU's recent implementation of the General Data Protection Regulation (GDPR) is just the latest development in this crucial area of law. Outside the EU, however, there is little uniformity in how different regions and countries protect personal data. To help make sense of this, Meritas® has produced this guide by leveraging its top quality member firms from around the world, specifically our firms in Asia Pacific, Europe and the USA. The guide employs a straightforward question-and-answer format to be as simple and as easy to use as possible. The authors hope that this guide will provide readers with a convenient and practical starting point to understand a complicated yet vitally important subject to businesses everywhere.

Special thanks go out to Meritas® Board Member Yao Rao (China), who was the inspiration behind this publication, as well as to Meritas® Board Member Darcy Kishida (Japan) and Eliza Tan (Meritas® Asia Regional Representative), who provided crucial support. Without their hard work and dedication, this global look at the critical issue of Data Privacy would not have been published.

ABOUT MERITAS®

Founded in 1990, Meritas® is the premier global alliance of independent law firms working collaboratively to provide businesses with qualified legal expertise. Our market-leading member firms offer a full range of high-quality, specialized legal services, allowing you to confidently conduct business anywhere in the world.

As an invitation-only alliance, Meritas® firms must adhere to our uncompromising service standards to retain membership status. Unlike any other network or law firm, Meritas® collects peer-driven reviews for each referral, and has for more than 25 years.

7,500+ EXPERIENCED LAWYERS

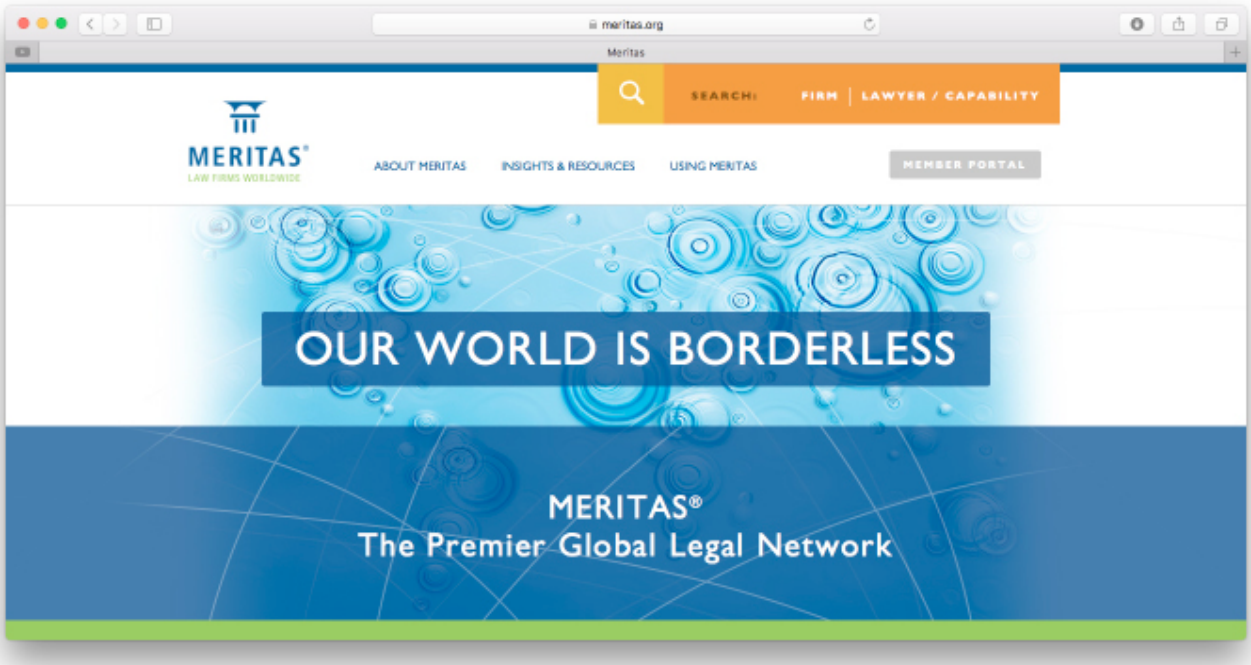
90+ COUNTRIES

180+ LAW FIRMS

240+ GLOBAL MARKETS

Using this exclusive ongoing review process, Meritas® ensures quality, consistency and client satisfaction.

With 180+ top-ranking law firms spanning more than 90 countries, Meritas® delivers exceptional legal knowledge, personal attention and proven value to clients worldwide.



For more information visit:

MERITAS®
LAW FIRMS WORLDWIDE

www.meritas.org

MERITAS®
LAW FIRMS WORLDWIDE

PHILIPPINES

FIRM PROFILE:

ACCRALAW®

Angara Abello Concepcion Regala & Cruz Law Offices (ACCRALAW) is a leading full service Firm with about 150 lawyers. For 2017, it was recognized as an Outstanding Firm by Asialaw Profiles, Top Tier by the Legal 500, and Top Ranked by Chambers, Asian Mena Counsel, and Asian Business Law Journal. Its main offices are located at the ACCRALAW Tower in the newly developed Bonifacio Global City in Metro Manila. It has full service branches in the thriving commercial centers of Cebu City in the Visayas and Davao City in Mindanao. The Firm has an excellent track record in handling diverse, significant, and complex business projects and transactions for both local and multinational clients, and has been involved in landmark litigation cases.

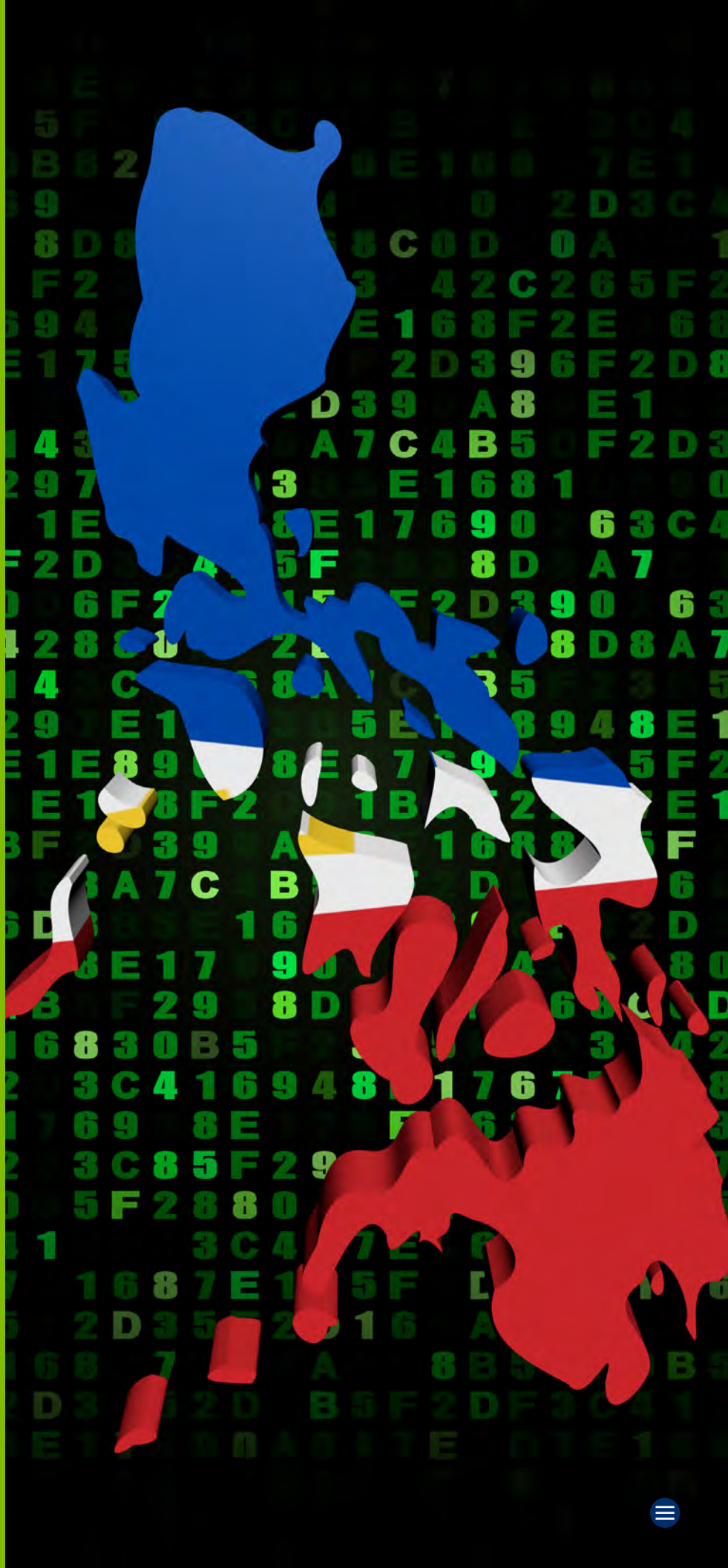
ACCRALAW's clientele represents the full spectrum of business and industry, and includes professional organizations and individuals. Servicing the Firm's clients are seven practice departments and its two branches, which offer timely, creative, and strategic legal solutions matched with cost-efficient administration and expert handling of clients' requirements.

CONTACT:

EMERICO O. DE GUZMAN
eodeguzman@accralaw.com

REGINA PADILLA-GERALDEZ
rpgeraldez@accralaw.com

+63 2 830 8000
www.accralaw.com



Introduction

The Data Privacy Act of 2012 or Republic Act No. 10173, with its Implementing Rules and Regulations, was promulgated in response to the freer exchange of personal data in the global stage and the setting of international standards for data protection. Prior to the Act, without so much as regulatory oversight for data collectors or protective measures for the data subject, the wealth of personal data available is subject to abuse and misuse — from the unmitigated use of contact details for purposes beyond those initially contemplated, to identity theft or security breaches of corporate data — to the detriment of the data subject's constitutionally guaranteed right to privacy. As this is a relatively new law in the Philippines and while initial enforcement measures have been implemented by the National Privacy Commission, it remains to be seen how robustly this new area of law will develop in the country.

1. What are the major personal information protection laws or regulations in your jurisdiction?

The governing law on personal information protection in the Philippines is the Data Privacy Act of 2012 or Republic Act No. 10173, together with its Implementing Rules and Regulations.

2. How is personal information defined?

Personal information is defined as any information, whether recorded in a material form or not, from which the identity of an individual is apparent by the entity holding the information.[1] For example, if the data collected pertains to his birthdate, address, Social Security number, or employee number, even if the individual is not explicitly named, then each data point (since the identity of the individual will be apparent when these data points are taken in consideration with each other) will be considered as personal data and, thus protected by the Data Privacy Act.

3. What are the key principles relating to personal information protection?

Processing of personal information must adhere to the general principles of transparency, legitimate purpose, and proportionality. For example, if the personal data of an individual is being collected for purposes of a conducting a contest wherein an individual will win a raffle prize of a store, then the data subject must be informed that his data is being collected and processed only for the said purpose and will be retained by the store for only as long as necessary to fulfill the contest. The data must not be used for any other purpose (e.g., marketing other products of the store) or kept longer than necessary (e.g., an indefinite period after the contest). The data collected must also be proportionate to the purpose. For example, if the purpose of collecting the data is to identify the winner of the contest, then the individual's name, birthdate, and address should suffice. Considering the purpose of the data collection, there is no need to collect the individual's mother's name, educational attainment, and his current employer, and so doing will violate the principle of proportionality of the Data Privacy Act.

4. What are the compliance requirements for the collection of personal information?

The processing of personal information is permitted if not prohibited by law and, generally, when the data subject has given his or her consent. The Data Privacy Act, however, recognizes situations wherein the nature or exigencies of the situation may not accommodate a situation wherein the individual can give his consent but his or her personal data still needs to be processed.[2] A good example of this will be a situation wherein the data subject's health is in danger and the data subject cannot give his or her consent in the form that the law requires (i.e., written). The Data Privacy Act, among other situations, recognizes this exception and allows for processing of personal data even without the data subject's consent.

5. What are the compliance requirements for the processing, use and disclosure of personal information?

Personal information controllers and personal information processors shall register with the National Privacy Commission their data processing systems or automated processing operations, subject to notification, if it employs at least two hundred fifty (250) employees, or if there is risk to the rights and freedoms of data subjects, or the processing is not occasional, or the processing includes sensitive personal information of at least one thousand (1,000) individuals.

In complying with the DPA-IRR's organizational security measures, the personal information controller must first:

(1) Have a compliance officer or data protection officer who shall ensure compliance with applicable rules and regulations for the protection of data privacy and security;

(2) Have data protection policies which provide for organizational, physical, and technical security measures;

(3) Maintain records that sufficiently describe its data processing system and identify the duties of individuals who have access to personal data;

(4) Hold capacity building, orientation, or training programs for employees who have access to personal data regarding privacy or security policies;

(5) Develop and implement procedures for collecting and processing personal data, access management, system monitoring, and protocols to follow during security incidents or technical problems, for data subjects to exercise their rights, and for a data retention schedule; and

(6) Ensure its contracts with personal information processors also implement the security measures required by the Data Privacy Act of 2012 and its IRR. [3]

Next, in complying with the DPA-IRR's physical security measures, the personal information controller must:

(1) Have policies/procedures to monitor and limit access to, and activities in, room, workstation or facility (including guidelines on use of and access to electronic media);

(2) Design office space and work stations to ensure privacy of processors of personal data;

(3) Define a clear description of duties, responsibilities and work schedules to processors of personal data to ensure only individuals actually performing duties are in the room at the given time;

(4) Implement policies and procedures on the transfer, removal, disposal, and re-use of electronic media; and

(5) Establish policies and procedures on the prevention of the mechanical destruction of files and equipment.[4]

Lastly, in complying with the DPA-IRR's technical security measures, the personal information controller must establish the following:

(1) A security policy with respect to processing personal data;

(2) Safeguards to protect computer networks against unauthorized access or to ensure data integrity and functioning of the system;

(3) The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;

(4) Regular monitoring for security breaches, accessing vulnerabilities, and preventive, corrective, and mitigating action against data breaches;

(5) Ability to restore availability and access to personal data in a timely manner;

(6) Processes for testing the effectiveness of security measures; and

(7) Encryption of personal data during storage, transit, authentication process, or any measure that controls and limits access.[5]

6. Are there any restrictions on personal information being transferred to other jurisdictions?

In cases of "data sharing" agreements, a disclosure or transfer must have been upon the instructions of the personal information controller concerned.

The term excludes "outsourcing", or the disclosure or transfer of personal data by a personal information controller to a personal information processor.[6]

The DPA-IRR provides "General Principles for Data Sharing" and allows processing of personal data collected from a party other than the data subject if the data subject's *informed* consent is obtained.[7] Specifically, the data subject must be informed of the identity of the personal information controller, the purpose of the data sharing, the categories of data that will be collected, the intended recipient of the data, and his rights over his personal data. For example, if the data subject's personal data is collected by his Philippine employer, who is part of an affiliate of companies located in multiple jurisdictions, if the employer decides to transfer his data for storage to one of the affiliates located elsewhere, then the employer must first obtain the data subject-employee's informed consent before doing so.

7. What are the rights of an individual whose personal information is collected? Can he/she withdraw the consent to the retention of his/her personal information by a third party, and if so, how?

The rights of an individual whose personal information is collected, also known as the data subject, are: to be informed that his data is being processed, to know the extent of the processing of such data (e.g., scope, purpose, to whom the data may be disclosed, period for storage), to know their rights to access and correction over the data, to have reasonable access to the data, to dispute inaccuracies or errors in their data, to suspend the destruction of their data, and to be indemnified for damages due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.[8]

A data subject may withdraw the consent to the retention of his/her personal information by a third party,[9] although there is no specific process given in the DPA-IRR on withdrawing consent.

8. Is an employee's personal information protected differently? If so, what's the difference? Apart from the personal information of employees, are there any other types of personal information that receive special protection?

Apart from exempting personal information which is necessary and desirable in the context of an employer-employee relationship from the requirement of prior notification before amendment (specifically as to any of the information listed under **Section 16 b of the Data Privacy Act**), an employee's personal information is not treated differently from that of the treatment accorded to personal information in general. However, a class of information that receives special protection is called sensitive personal information, wherein, among others, consent of the data subject must be specific to the purpose of processing.[10] Sensitive personal information refers to personal information:

(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or **current** health records, licenses or its denials, suspension or revocation, and tax returns; and

(4) Specifically established by an executive order or an act of Congress to be kept classified. [11]

For example, in interviewing applicants for a job, it is not enough to secure the data subject's general consent to collect their personal data and then include their Social Security or Tax Identification number in the collection and processing. The data subject-applicant must be informed, prior to consenting, that his personal and sensitive personal information will be collected and processed for determining his qualifications for the job and

to process employment-related requirements should he or she accept the job offer.

9. Which regulatory authorities are responsible for implementation and enforcement of personal information protection laws in your jurisdiction?

The National Privacy Commission is an independent body tasked to administer and implement the provisions of the Data Privacy Act, and to monitor and ensure compliance of the country with international standards set for data protection.

10. Are there any penalties, liabilities or remedies if any of the personal information protection laws is violated?

Yes, there are penalties in the form of fines ranging from One Hundred Thousand Pesos (Php100,000.00) to Five Million Pesos (Php5,000,000.00) and imprisonment ranging from six (6) months to six (6) years depending on the type of violation committed.[12]

11. Is your jurisdiction planning to pass any new legislation to protect personal information? How is the area of personal information protection expected to develop in your jurisdiction?

Apart from the Data Privacy Act and the DPA-IRR, no further legislation is in contemplation in the Philippines relating to personal information protection. However, it is worthy to note that the National Privacy Commission regularly issues Circulars and Advisories to further clarify the implementation of and for guidance of the public as to complying with the Data Privacy Act and the DPA-IRR. The National Privacy Commission likewise issues Advisory Opinions for queries, which it publishes on its website and is considered to have, at the very least, persuasive effect.

Conclusion

Based on the issuances of the National Privacy Commission, a company that wishes to comply with the provisions of the Data Privacy Act of 2012 must focus on the following requirements:

(1) Appoint a data protection officer who will ensure compliance with the Data Privacy Act of 2012 and the DPA-IRR;

(2) Conduct a Privacy Impact Assessment (with a template available at https://privacy.gov.ph/wp-content/uploads/NPC-PIA-Template-v2.pdf);

(3) Create a Privacy Manual which contains the protocols for each step in processing personal information with the goal of complying with complying with the Data Privacy Act of 2012, the DPA-IRR, and the issuances of the National Privacy Commission;

(4) Implement a privacy and data protection policy; and

(5) Install and maintain a breach reporting protocol.

Finally, in reference to the registration requirements for a personal information controller and personal information processors, as mandated by National Privacy Commission Circular 17-01, certain sectors or institutions wherein processing of personal data is likely to pose a risk to the rights and freedoms of data subjects and/or where the processing is not occasional, are required to register their data processing systems. While Phase 1 and 2 of the registration process has already lapsed (9 September 2017 and 9 March 2018, respectively), it is nevertheless prudent for companies who are mandated to register to comply, as the Commission will still accept late registrants, although they will be included in the list of priority organizations for a data privacy compliance check.

Authors: Neptali B. Salvanera and Franchesca C. Gesmundo.

Footnotes

[1]/ An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012] Republic Act No. 10173, Section 3 (g) (2012).

[2]/ *Id.* Section 12.

[3]/ National Privacy Commission, Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012", Rule VI, Section 26 (2016) (hereafter, "DPA-IRR").

[4]/ *Id.* Rule VI, Section 27.

[5]/ *Id.* Rule VI, Section 28.

[6]/ *Id.* Rule I, Section 3, f.

[7]/ *Id.* Rule IV, Section 20.

[8]/ Data Privacy Act of 2012, Section 16.

[9]/ DPA-IRR, Rule IV, Section 19 a 1 and b 1.

[10]/ *Id.* Section 13.

[11]/ *Id.* Section 3 (l).

[12]/ *Id.* Sections 25-33.

Prepared by Meritas Law Firms

Meritas is an established alliance of 180+ full-service law firms serving over 240 markets – all rigorously qualified, independent and collaborative. Connect with a Meritas law firm and benefit from local insight, local rates and world-class service.

www.meritas.org enables direct access to Meritas law firms through a searchable database of lawyer skills and experience.

MERITAS®
LAW FIRMS WORLDWIDE

www.meritas.org

800 Hennepin Avenue, Suite 600
Minneapolis, Minnesota 55403 USA
+1.612.339.8680