



汇衡律师事务所
HHP ATTORNEYS-AT-LAW

个人信息保护全球指南

第二版

菲律宾



MERITAS[®]
LAW FIRMS WORLDWIDE



汇衡律师事务所
HHP ATTORNEYS-AT-LAW

个人信息保护全球指南

亚太、欧洲和美国



编辑：Dennis Unkovic

du@muslaw.com

电话：+1 (412) 456 2833

Meyer, Unkovic & Scott
律师事务所

www.muslaw.com

一年前，为响应人们对欧盟《一般数据保护条例》（GDPR）的广泛兴趣，Meritas律师事务所联盟制作了《个人信息保护全球指南》。GDPR引发了一场全球运动，来应对那些认为有必要保护并加强对其隐私信息保护程度的个人需求。这场运动是在全球数亿人遭受大规模数据泄露影响之际出现的，涉及Marriott、Twitter、Under Armour、Facebook等公司，以及最近的Capital One，可能已经影响到了1亿多用户。2018年，共有1244起影响到美国公司和消费者的数据泄露事件被公开报道，仅这些违规行为就暴露了约4.46亿条个人信息。

由于这些事件正日益频繁地上演，Meritas在此很荣幸能发布这本深受好评的刊物的第二版。此次的新版本，增加了关于欧洲的章节篇幅，以突显各个欧洲国家对GDPR的不同看法。此外，所有章节的撰稿人都在第11个问题中增补了隐私权的最新进展。

我们希望您能认可《个人信息保护全球指南（第二版）》。如果您在这一重要问题上希望获取更具体的意见，请随时与本指南列出的任何一家Meritas成员律所联系。

特别感谢Meritas董事会成员饶尧（中国）、Darcy Kishida（日本）、Jeffrey Lim（新加坡），以及Meritas亚洲区域代表Eliza Tan，他们为这本指南的制作提供了关键支持。没有他们的辛苦工作和付出，就不会有这本以全球视角看待数据隐私关键问题的刊物出版。

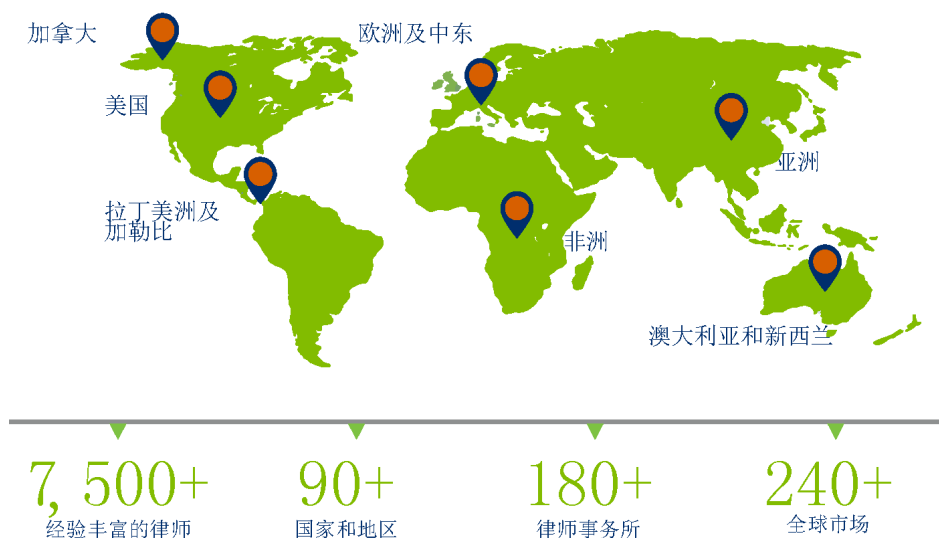


汇衡律师事务所
HHP ATTORNEYS-AT-LAW

关于MERITAS®

Meritas成立于1990年，是领先的全球性独立律师事务所联盟，致力于通过协同工作为企业提供合格的法律专业服务。我们市场领先的成员事务所提供全方位、高质量的专业法律服务，让您能够在世界上的任何地方自信地开展业务。

作为一个仅能通过邀请加入的联盟，Meritas的事务所必须遵守我们严格的服务标准方能保留成员资格。与其他组织或律师事务所不同，Meritas对成员所的每一次推荐均收集同行评价意见，这种做法已有超过25年的历史。

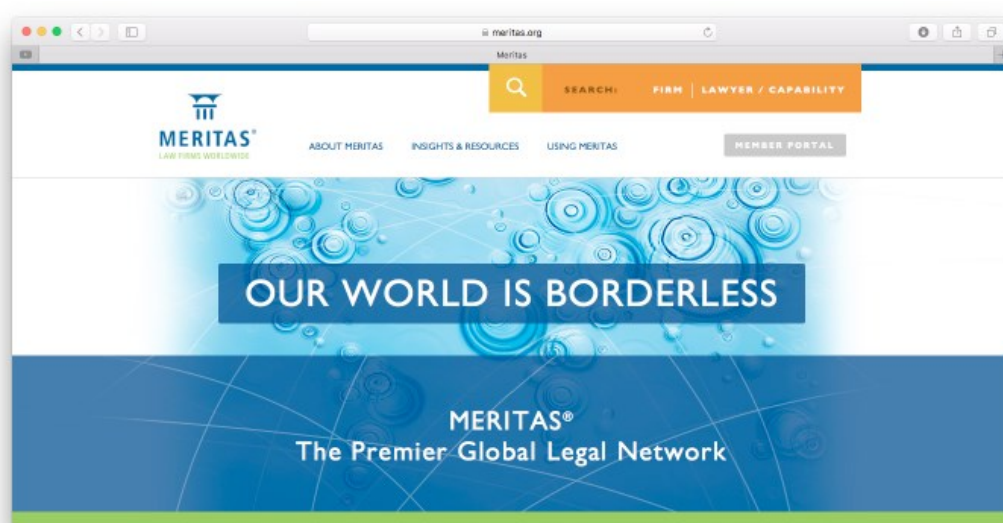




汇衡律师事务所
HHP ATTORNEYS-AT-LAW

利用这种独特的持续审核程序，Meritas保证质量、一致性及客户满意度。

Meritas拥有遍布超过90个国家和地区的180多家顶级律师事务所，为全球客户提供卓越的法律服务、个性化的关注以及行之有效的价值。



欲知更多信息，请访问：

www.meritas.org



亚洲



Meritas亚洲数据安全与隐私项目组是成员律所领导的项目组，聚焦于亚洲复杂的多辖区法律和监管环境中的数据保护、隐私及数据安全问题。

随着亚洲的繁荣发展以及与全球经济的联系日益紧密，每个独特的司法管辖区都为其法律体系提供了强大的支持，该项目组整合了专业知识和资源，从而提供了一个强大的平台来满足客户的国内和跨境需求。

通过联系Meritas亚洲数据安全和隐私项目组，客户和其他成员律所可以获得专业知识，包括：

- 建立符合当地法规的数据保护/隐私治理框架；
- 执行数据保护影响评估；
- 开展和执行数据保护和隐私影响评估及审计；
- 关于数据传输或数据出口管制的建议和实际解决办法；
- 数据泄露的咨询支持；
- 在数据分析和相关项目中使用个人数据的建议。

亚洲



以下成员所可以为您在亚洲的数据保护需求提供帮助：

中国

饶尧

汇衡律师事务所

上海

yao.rao@hhp.com.cn

www.hhp.com.cn

刘洪川

世泽律师事务所

北京

hongchuan_liu@broadbright.com

中国香港

黄永昌

何耀棣律师事务所

中国香港

philipwong@gallantho.com

印度

Chakrapani Misra

Khaitan & Co.

班加罗尔、加尔各答、孟买、新德里

chakrapani.misra@khaitanco.com

www.Khaitanco.com

印尼

Milanti T. Kirana

HHR Lawyers

雅加达

milantikirana@hhrlawyers.com

www.hhrlawyers.com

日本

小川浩贤

小岛国际法律事务所

东京

ogawa@kojimalaw.jp

www.kojimalaw.jp/en

菲律宾

Emerico de Guzman

ACCRA LAW

宿务、达沃、马尼拉

eodeguzman@accralaw.com

www.accralaw.com

新加坡

Joyce A. Tan

Joyce A. Tan & Partners

新加坡

joyce@joylaw.com

www.joylaw.com

泰国

Palawi Bunnag

ILCT Advocates & Solicitors

曼谷

palawib@ilct.co.th

www.ilct.co.th

越南

Nhut Nguyen

Russin & Vecchi

胡志明市

nhmnhut@russinvecchi.com.vn

www.russinvecchi.com

菲律宾



联系人

EMERICO DE GUZMAN

eodeguzman@accralaw.com

ANA LOURDES TERESA
ARNALDO - ORACION

aaoracion@accralaw.com

+63 2 830 8000

www.accralaw.com



Angara Abello Concepcion Regala & Cruz 律师事务所 (ACCRALAW) 是一家处于领先地位并可提供全方位服务的律师事务所，拥有约150名律师。在2019/2018年度，ACCRALAW 被Asialaw Profiles评为“2019年杰出律师事务所”，被Asialaw Regional Awards评为“2019年度最佳菲律宾律师事务所”并获“最佳客户服务奖”，获Benchmark Litigation Asia Pacific “2019年度律所大奖”，被Legal 500评为顶级律所、领先律所，被钱伯斯亚太评为顶级律所，被《亚洲法律顾问》评为“2018年度最佳律所”，并被《亚洲商业法律月刊》评为“2018年度菲律宾最佳律所”。ACCRALAW总部位于马尼拉大都会新开发的伯尼法西奥环球城中的ACCRALAW大厦。ACCRALAW在繁荣的商业中心米沙鄢群岛的宿务市和棉兰老岛的达沃市均设有提供全方位服务的分所。

在为本国和跨国客户处理各种重要、复杂的商业项目和交易方面，该事务所成绩斐然，其中不乏一些具有里程碑意义的诉讼案件。

ACCRALAW的客户涵盖了商业和工业的各个领域，包括专业机构和个人。该事务所有七个事务部门和两个分所为客户提供服务，配有成本效益管理和处理客户需求的专家，为事务所的客户提供了及时、富有创造性和战略性的法律解决方案。

导言

为应对全球范围内越来越自由的个人数据交换并对数据保护国际标准的制定作出响应，菲律宾于2012年颁布了《数据隐私法（2012年）》（或《第10173号共和国法案》，“DPA”）及其实施细则和规定。在此之前，菲律宾并没有对于个人数据处理者的集中监管或对数据主体的全面保护措施，当时，大量的个人数据受到滥用和不当使用——从超出原本预计目的的无节制使用和分享联系信息，到身份窃取或安全入侵——直到数据主体受宪法保障的隐私权受损。早在2006年，菲律宾贸易和工业部（DTI）就发布了关于“个人数据保护指南”的第8-2006号DTI行政命令，这是《数据隐私法》的起源。DTI的发布是仿效欧盟（EU）1995年《数据保护指令》（官方指令95/46/EC）的模式，该指令是当前欧盟《一般数据保护条例》（GDPR）的前身。因此，菲律宾的《数据隐私法》深深根植于欧盟《一般数据保护条例》所倡导的标准和原则。

1. 您所在的法域中主要的个人信息保护法律或法规有哪些？

菲律宾关于个人信息保护的管辖法律是《数据隐私法（2012年）》/《第10173号共和国法案》及其实施细则和规定。除了《数据隐私法》及其实施细则和规定，国家隐私委员会作为负责管理菲律宾隐私法律的主要政府机构，发布了进一步完善并实施《数据隐私法》及其实施细则和规定的通告和建议。

2. 个人信息是如何定义的？

“个人信息”被定义为持有该信息的实体可以从中明显识别出个人身份的任何信息，无论是否以实物形式记载。¹ 例如，如果被收集的数据涉及其家庭住址、电话号码或雇员编号，即便该自然人并未被明确指名，每一个数据点（鉴于当将这些数据点相互结合考虑时，自然人身份会变得显而易见）都将被认定为个人信息，并因此受到《数据隐私法》的

保护。根据此法律定义，与法律实体（例如公司、企业和合伙企业）有关的信息不受法律规制。尽管“公司信息”是被排除在《数据隐私法》的范围之外的，但是如果与法人实体有关的记录或文件包含个人信息（例如，公司注册文件中的公司注册人或公司管理人员的姓名和联系方式），那么这部分包含个人信息的记录或文件仍应被视为《数据隐私法》所涵盖的范围。

从“个人信息”的范畴来看，我们的法律划定了两组“特殊”的个人信息——“特许保密信息”和“敏感个人信息”。“特许保密信息”的定义是“指根据《法院规则》和其他有关法律构成特许保密通信的任何形式的数据”。² 根据《法院规则》第24章第130条，以下内容构成“特许保密通信”：（1）夫妻或配偶的交流；（2）律师与委托人的通信；（3）医患沟通；（4）牧师与忏悔者的交流；（5）公职人员通信。

同时，“敏感个人信息”是指如下个人信息：

（1）关于自然人的种族、民族血统、婚姻状况、年龄、肤色以及宗教、哲学或政治信仰；

（2）关于自然人的健康、教育、基因或性生活，或实施或被指控实施任何违法行为的任何程序、该等程序的处理结果或任何法院在该等程序中判处的刑罚；

（3）政府机构向自然人签发的特有信息，包括但不限于社会保障号码、过去或目前的健康记录、执照或其驳回、中止或撤销信息以及税费返还；及

（4）由行政命令或议会法案特别建立的、需要秘密保管的信息。³

《数据隐私法》的上述列表详尽无遗地列出了构成“敏感个人信息”的内容，未包含在内的那些个人数据被视为“非敏感”数据，但仍然是《数据隐私法》所保护的“个人信息”（如姓名、联系方式，如电话号码、电子邮件地址等）。“特许保密信息”和“敏感个人信息”在《数据隐私法》项下是被同等对待的。

3. 有关个人信息保护的关键原则有哪些？

和《一般数据保护条例》拥护的原则相似，个人信息的处理行为必须遵守透明性、合法目的和相称性的一般原则。例如，如果出于举办比赛的目的而收集自然人的个人数据且自然人将由此赢得某一商店的抽奖奖品，那么必须告知数据主体其数据系仅出于上述目的而被收集和处理，并且该等数据将由商店保留，保留时间仅限于满足比赛要求所需的时间。该等数据不得用于其他任何目的（例如，推销商店的其他产品）或保留超过必要期限（例如，比赛后的一段不确定的期限）。

被收集的数据还必须与向数据主体宣称的目的相称。例如，如果收集数据的目的是识别比赛获胜者的身份，那么个人的姓名和联系信息就足够了。

《数据隐私法》中透明性原则的特点是需要获得数据主体的明示同意或处理个人信息的有效法律依据。首先，必须告知数据主体其个人信息将如何被使用或“处理”，包括涉及的各方（如数据控制者、数据处理者、第三方），需要此类个人信息的目的，个人信息应被保留多长时间，为保护数据应采取的适当安全措施，以及在数据主体有任何顾虑时如何联系数据控制者的详细联系方式。如果缺失上述任何行为，那么根据《数据隐私法》，“个人信息的处理”通常可以被视为未经授权。

4. 收集个人信息的合规要求有哪些？

未被法律禁止的个人信息处理行为均是被允许的，通常而言，当数据主体已经明确、明示同意时，是可以处理个人信息的。但是，根据情况的性质和紧急程度，《数据隐私法》规定了一些不适合由个人作出同意但其个人数据仍需要被处理的情形。⁴ 例如，当数据主体的健康受到威胁且数据主体无法以法律要求的形式（即：书面形式）作出同意的情形就是一个典型的例子。对此，《数据隐私法》规定了这一例外并允许在即使没有数据主体同意的情形下仍可处理个人数据。

《数据隐私法》中概述的上述豁免情况仅在此类处理个人信息的情况下，免除同意要求，但并不免

除数据控制者和/或数据处理者遵守《数据隐私法》的其余要求和标准，例如但不限于实施合理且充分的安全措施以保护个人信息的“私密性、完整性和可用性”。

5. 处理、使用和披露个人信息的合规要求有哪些？

一般来说，个人数据控制方和个人数据处理方需要任命或指定一名数据保护专员。对于某些个人数据控制者和个人数据处理者，需要向国家隐私委员会登记其数据保护专员和数据处理系统。需要向国家隐私委员会登记的个人信息控制者和个人数据处理者如下：

（1）雇佣至少二百五十（250）名员工；或

（2）不管雇员人数多少，从事可能对数据主体的权利和自由构成风险的操作或个人信息处理活动的，或此类处理行为不是偶然性的；或

（3）处理至少一千（1000）名自然人的敏感个人信息；或

（4）不管雇员人数或数据主体多少，只要是被全国隐私委员会列为“关键部门”的部门/行业，如银行和非银行金融机构；医院、医疗中心和与健康有关的组织；中小学校和大学；研究机构；业务流程外包公司（包括“共享服务”的提供商或拥有“垄断市场”的公司）；电信公司。

无论是否在全国隐私委员会登记要求的范围内，所有的个人数据控制者和个人数据处理者都必须实施适当和合理的安全措施，以确保个人信息的“私密性、完整性和可用性”。《数据隐私法》及其实施细则和规定列举了这些具体的安全措施，并将其分为三（3）组，即：（1）组织性的；（2）物理性的；和（3）技术性的安全措施。

个人数据控制者和个人数据处理者必须实施的组织性安全措施包括以下：

（1）拥有一名合规专员或数据保护专员，其应当

确保遵守适用的数据隐私与安全保护规定与条例；

（2）构建数据保护政策，提供组织性、物理性和技术性安全措施；

（3）保存足以描述其数据处理系统并识别有权访问个人数据的人员职责的记录；

（4）为有权访问个人数据的员工组织关于隐私或安全政策方面的能力建设、训练或培训项目；

（5）为数据主体行使其权利并为数据保留计划、开发并实施收集和处理个人数据、访问管理、系统监控的程序，以及发生安全性事件或技术问题时需遵循的方案；及

（6）确保与个人数据处理者（即，第三方供应者或销售者）的合同亦采取《数据隐私法》及其实施细则和规定要求的安全措施。⁵

个人数据控制者和个人数据处理者必须实施的物理性安全措施包括以下：

（1）建立制度/流程以监督和限制房间、工作区或设施的访问权限及其中的活动（包括关于使用和访问电子媒体的指南）；

（2）对办公空间和工作区域进行设计以确保个人数据处理者的隐私；

（3）定义一个适用于个人数据处理者的职责、责任和工作时间表方面的明确描述，以确保只有实际履行职责的自然人能够在规定的时间内处于该房间内；

（4）实施电子媒体转移、清除、处理和再使用的政策和程序；及

（5）建立预防文件和设备发生机械性损坏的政策和程序。⁶

最后，个人数据控制者和个人数据处理者必须实施的技术性安全措施包括以下：

（1）确立关于处理个人数据的安全政策；

（2）确立保护计算机网络抵御未经授权的访问或确保系统的数据完整性和功能的防护措施；

（3）确保和保持其处理系统和服务的保密性、完整性、可用性和恢复性；

（4）建立对安全入侵行为、访问弱点的定期监控，以及对数据入侵行为采取预防性、纠正性和缓和性行动；

（5）提高以及时方式恢复个人数据可用性和可访问性的能力；

（6）确立检测安全措施有效性的流程和规约；及

（7）实施在存储、传输、认证过程中对个人数据进行加密或采取任何控制和限制访问的措施。⁷

6. 是否存在转移个人信息至其他法域的限制？

一般而言，《数据隐私法》不限制个人信息的跨境转移，前提是：（1）相关数据主体已被充分告知/通知此类转移，并同意此类传输；（2）如果个人信息应被转移给第三方，则必须签订相关协议（无论是“外包/分包”协议还是“数据共享”协议）。关于第二项中提及的协议，《数据隐私法》及其实施细则和规定要求包括“强制性条款”，以确保第三方遵守《数据隐私法》的规定并实施适当的安全措施。根据《数据隐私法》，属于同一集团公司的子公司、关联公司或实体被视为彼此的“第三方”。

7. 被收集个人信息的个人拥有哪些权利？他们可否撤销对第三方保留他们个人信息的同意？以及如果可以，如何撤销？

个人信息被收集或处理的自然人（亦即所谓的数据主体）的权利有：被告知其数据正在被处理的权力，了解该等数据处理程度（例如，范围、目的、数据可能向谁披露、存储期限）的权利，了解其访

问和修正数据的权利，对数据拥有合理的访问权限的权利，对其数据中的不准确或错误提出异议的权利，暂停销毁其数据的权利，就因该等个人信息的不准确、不完整、过时、错误、或非法获取或未经授权地使用个人信息的行为而遭受的损失获得赔偿的权利。

数据主体可撤回对于第三方⁹保留其个人信息的同意，尽管《数据隐私法》及其实施细则和规定并未就撤回同意规定具体的流程。⁸

8. 雇员的个人信息保护是否有所不同？如有不同，有哪些不同？除了雇员的个人信息，是否有受特殊保护的其他类型的个人信息？

在雇主与雇员关系情境下，豁免个人信息在修改之前需要事先通知的要求是必要且可取的，除此之外，雇员的个人信息在处理时与通常的个人信息没有什么不同。

9. 在菲律宾什么监管机构负责实施和执行个人信息保护法律？

国家隐私委员会是一个独立机构，职责在于管理和实施《数据隐私法》及其实施细则和规定，监督并确保国家符合数据保护的国际标准。

10. 如果违反任何个人信息保护法律，是否有任何处罚、责任或救济？

处罚形式包括十万（100,000.00）菲律宾比索至五百万（5,000,000.00）菲律宾比索之间不等的罚金处罚以及六（6）个月至六（6）年之间不等的监禁处罚，具体取决于实施的违法行为的类型。¹⁰除了罚款和监禁（两者都是强制性的）之外，数据主体还可以寻求民事损害赔偿（如实际损害赔偿、精神损害赔偿、惩戒性损害赔偿等）。

11. 菲律宾最近在数据隐私/数据保护方面有何显著进展？例如，菲律宾是否正在计划通过任

何新的立法以保护个人信息？个人信息保护领域在菲律宾预计会如何发展？

除《数据隐私法》及其实施细则和规定外，菲律宾未打算进一步制定关于个人信息保护的立法。然而，根据法律授权，国家隐私委员会定期发布通知和建议以进一步明确《数据隐私法》及其实施细则和规定的实施情况。同样，国家隐私委员会会在其网站上就问题咨询发布，至少被认为是具有说服力的咨询意见。最近，国家隐私委员会发布了《合规性检查规则》，概述了网络隐私扫描的程序、相关实体提交的合规性文件以及现场合规性检查。此外，国家隐私委员会还明确宣布，律师和医务人员等单一专业从业人员必须向国家隐私委员会登记，国家隐私委员会为满足这一要求，制定了单独的登记程序和表格。

结论

为确保所有个人和实体（即个人数据控制者和个人数据处理者）遵守《数据隐私法》及其实施细则和规定以及国家隐私委员会发布的要求，国家隐私委员会阐明了其所称的“隐私合规五大支柱”，即：

1. 任命一名数据保护专员；
2. 进行隐私影响评估；
3. 创建隐私手册，内容包括处理个人信息的每一步骤方案，目的是遵守现行隐私法律和法规；
4. 实施隐私和数据保护政策；
5. 安装并维护违法行为报告规程。

最后，关于登记的要求，涵盖的个人数据控制方和个人数据处理方仍然可以在国家隐私委员会登记（数据保护专员的登记——登记程序的第一阶段）；延迟登记不会被处罚。然而，在2019年，数据处理系统登记——登记程序的第二阶段仍处于被国家隐私委员会暂停的状态，需等待其另行通知。

脚注

1. 关于保护政府和私人部门信息和沟通系统中自然人个人信息、为此目的创建国家隐私委员会和出于其他目的的法案，《数据隐私法（2012年）》/《第10173号共和国法案》第3(g)条，2012年。
2. 同上，第3(k)条。
3. 同上，第3(l)条。
4. 同上，关于处理“个人信息”的第12条（即那些未归类为“敏感个人信息”和“特许保密信息”的信息）；关于处理“敏感个人信息”和“特许保密信息”的第13条。
5. 国家隐私委员会《第10173号共和国法案（即“数据隐私法（2012）”）实施细则和规定》，细则六，第26条（2016年）（“DPA-IRR”）。同上，细则六，第28条。
6. 同上，细则一，第3,f条。
7. 同上，细则六，第27条。
8. 《数据隐私法（2012年）》，第16条。
9. DPA-IRR，细则六，第19 a 1和b 1条。
10. 同上，第25-33条。



汇衡律师事务所

HHP ATTORNEYS-AT-LAW

中国上海市黄浦区湖滨路168号

无限极大厦（企业天地三号楼）1818室

电话：+86-21-5047 3330

传真：+86-21-5047 0264

官网：www.hhp.com.cn

邮箱：office@hhp.com.cn



MERITAS[®]

LAW FIRMS WORLDWIDE

www.meritas.org

亨内平大街800号，600室

明尼阿波利斯市

美国明尼苏达州 55403

+1.612.339.8680