个人信息保护全球指南

美国

第一版

MERITAS®
LAW FIRMS WORLDWIDE

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

在不是很久之前，“数据保护”意味着一个上锁的档案柜和一台良好的碎纸机。但在一代人的时间内，前述情况不复存在，数据保护从保管文件发展为保护几乎每种信息，无论是有形的还是以电子形式呈现的。虽然每个人都理解保护纸质文件意味着什么，但是形成对无形信息保护的概念却困难得多。更为糟糕的是，是，如今数据泄露可以造成比过去更为严重的后果。举例而言，对个人数据的不正当披露能轻易导致成身份盗用，而受害者事发前往往难以察觉该等犯罪行为。

随着技术的不断进步和世界的联系日益紧密，保护个人数据无疑比以往更加重要。对此，各国政府为跟上飞速变革的步伐已经开始关注相关立法。欧盟最近实施的《一般数据保护条例》（GDPR）正是这一关键法律领域的最新发展。然而，在欧盟之外，不同国家和地区保护个人数据的方式却不甚统一。为了便于理解这一问题，Meritas借助其世界各地顶尖品质的成员事务所，尤其是我们在亚太、欧洲和美国的事务所的力量制作了本指南。为了使用起来尽可能简单、容易，本指南采用直接式问答的形式。作者们希望，本指南将为读者提供一个便捷和实用的切入点来理解一项虽然复杂但却对各地业务都至关重要的主题。

特别感谢Meritas董事会成员饶尧（中国），是他为本指南的制作注入了灵感；并感谢Meritas董事会成员Darcy Kishida（日本）和Meritas亚洲区域代表Eliza Tan，二人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。

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。

7, 500+
经验丰富的律师

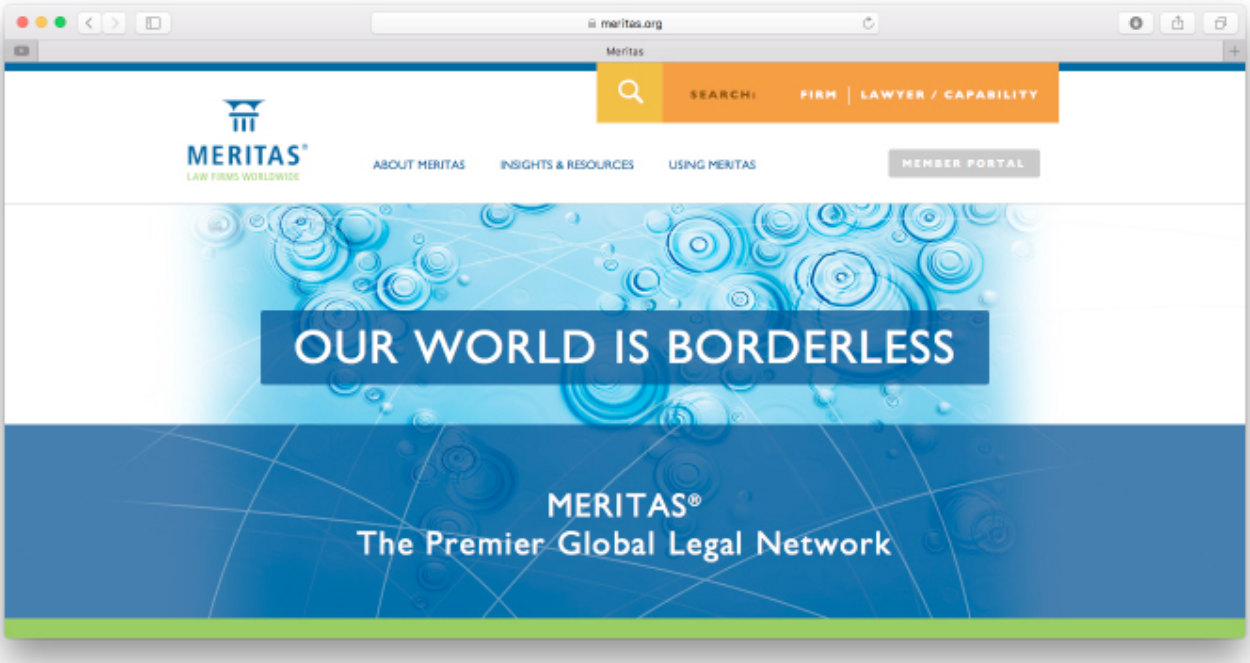
90+
国家和地区

180+
律师事务所

240+
全球市场

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知识、个性化的关注以及行之有效的价值。



预知更多信息，请访问：

MERITAS®

LAW FIRMS WORLDWIDE

www.meritas.org

MERITAS®
LAW FIRMS WORLDWIDE

美国

律师事务所简介：

MEYER UNKOVIC SCOTT
ATTORNEYS AT LAW

Meyer, Unkovic & Scott成立于1943年，是一家提供全方位服务的律师事务所，拥有包括财富100强公司、重要金融机构、商事企业和个人在内的各类客户。本所在为来自全球各地的客户处理国际事务方面具有丰富的经验。

我们就法律事务提供建议，包括构建不同商业交易架构、兼并和收购、外商直接投资、知识产权和数据保护、不动产和银行法、破产法、劳动法、国际法、移民问题、税务筹划和商事诉讼与仲裁。

我们努力理解每位客户的独特目标和需要。我们非常重视清晰明了、简明扼要和定期展开的沟通。

Dennis Unkovic自2015年4月至2018年5月任Meritas®的全球主席。自1999年10月11日起，Meyer, Unkovic & Scott就一直是Meritas®活跃成员。

联系人：

DENNIS UNKOVIC
du@muslaw.com

MICHAEL G. MONYOK
mgm@muslaw.com

+1-011-412-456-2800
www.muslaw.com

导言

在美国，数据保护是一个重要且不断演化的问题。国家层面和各州层面的各项法律法规对于个人信息的收集、存储和使用进行保护。在国家层面，有多个联邦机构负责执行适用法律法规，包括联邦贸易委员会（FTC）、卫生与公众服务部（DHS）和消费者金融保护局（CFPB）。各机构之间划分执行的职责源于缺少一部关于个人信息保护的单行的、综合性的法律。

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？

以下是与在美国进行商业运作最为相关的现行法律法规的概述：

- 《联邦贸易委员会法案》（《美国法典》第15卷第41-58节）：规定FTC管理欺诈性和不公平贸易活动的一般权限。FTC将其基本法解释为包含管理网络安全活动和未经授权披露个人信息行为的权限。联邦法院在FTC对Wyndham Hotels（温德姆酒店）提起的执行程序中确认了FTC的权限。FTC提起执行程序，主张温德姆酒店因未能实施合理的安全程序，而在三次单独的黑客攻击中将数十万顾客的支付卡信息不公平地暴露在黑客面前。为了解决这一诉讼，温德姆酒店支付了高昂的罚金。
- HIPAA法规（《联邦法规汇编》第45篇第160节）：该法规对于医院、医护人员、医生、医疗卫生所和上述机构的任何商业伙伴收集和使用受保护的健康信息进行管理。
- 《儿童在线隐私保护条例》（《联邦法规汇编》第16篇第312节FTC法规）：该条例禁止实施与收集、使用和/或披露互联网上来自或关于儿童的个人信息的不公平或欺诈性行为或活动。根据这一条例，父母有权控制关于其子女的何种信息可被收集。
- 消费者金融信息隐私法规（FTC法规，《联邦法规汇编》第16篇第313节）：根据FTC法规这一节的规定，金融机构需要告知消费者其隐私政策和实践。此外，条例描述了金融机构可能会向非关联第三方披露消费者非公开个人信息的情形。
- 保护客户信息的标准（《联邦法规汇编》第16篇第314节FTC法规）：FTC法规中规定的实体“应当开发、实施并维护按照一个或多个可立即使用的部分编写的包含管理、技术和物理防护的综合性信息安全程序”以保障客户信息的安全性、保密性和完整性。所覆盖的实体包括广义上的金融机构以及所覆盖实体的任何服务提供商。
- 《反垃圾邮件条例》（《联邦法规汇编》第16篇第316节FTC法规）：规定电子邮箱地址的收集和使用。
- 《电子通讯隐私法案》（《美国法典》第15卷第2510节和《计算机欺诈和滥用法案》（《美国法典》第18卷第1030节）：这些法律限制传输中或存储中的电子数据的拦截以及禁止未经授权的计算机访问。
- 各州隐私法律：几乎50个州都有法律规定要求对个人信息涉及安全攻击的情况向个人进行通知。

2. 个人信息是如何定义的？

个人信息的定义会由于适用的不同的法律或法规而不同。通常，这一术语系指单独或与其他信息结合可用于识别个人的信息。例如，FTC认为一个人的姓名、地址、社会安全号码、信用卡号码、账户信息和其他类似数据是“个人可识别信息”。许多州采用一种类似开放性解释的方式，即可用于识别个人身份的个人姓

名或额外的信息被视为个人信息。HIPAA法规适用于以任何形式，无论是电子的、纸质的或口头存储任何“个人的可识别健康信息”。法律法规中通常援引“客户”或“个人”，因此对个人信息的保护措施很可能同等适用于公民与非公民。此外，许多法规的目的在于保护与个人相关（而非与法人相关）的数据。

3. 有关个人信息保护的关键原则有哪些？

美国关于个人信息保护的关键原则是：（1）制定并遵守收集和使用客户信息的隐私政策；（2）使用合理防护措施保护个人或敏感信息；及（3）将攻击行为通知每一个其信息遭到泄露的个人。

“合理的”这一术语可能有些含糊，美国的联邦机构已经将国家标准与技术研究院制定的《网络安全框架》（“框架”；获取网址 <https://www.nist.gov/cyberframework>）作为官方政策。国家标准与技术研究院是一家推动创新与工业竞争力的联邦机构。框架由管理网络安全相关风险的标准、指引和最佳实践组成。对框架的遵循与FTC判断一家公司的行为是否构成欺诈性或不公平行为时使用的“合理性”标准相符合，亦满足了HIPAA的要求。例如在FTC提起的一次执行行动中，FTC主张Petco Animal Supplies（一家大型的国内零售连锁店）未能实施保护消费者信息的政策和程序。但如果该连锁店按框架的建议，建立有组织的信息安全政策本可以避免这一问题。

4. 收集个人信息的合规要求有哪些？

收集个人信息通常并不受到规制。在这方面，欧洲通过实施《一般数据保护条例》在规制个人信息收集方面遥遥领先于美国。不过，虽然不是一项强制要求，FTC在针对在线行为广告的自律原则中建议网页披露其数据收集实践并使客户能够选择退出。

5. 处理、使用和披露个人信息的合规要求有哪些？

如上所述，处理、使用和披露个人信息的合规要求取决于适用何种法律或法规。除大多数健康信息和一些金融信息外，并不禁止处理、使用和披露个人信息。就健康和金融信息而言，实体仅可在法规允许的情形下披露该等信息。例如，医生可将健康信息传递给保险公司。为了保证此类情形下信息传递的安全性，该等实体往往需要与接收方存在合同关系约定接收方同意受到与披露方相同的安全要求的约束。

6. 是否存在转移个人信息至其他法域的限制？

在转移个人信息至外国法域方面很少有限制。然而，实体可能仍会受到FTC对涉及转移至美国境外信息的行为的规制。例如，Facebook因允许英国的咨询事务所访问数百万美国的Facebook用户的资料而正在接受FTC的调查。Facebook的行为还会受到纽约州和马萨诸塞州检察官负责的调查。

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？

个人对其信息不享有具体权利。并且，由于保留信息不需要取得同意，因此个人无法撤销同意。尽管如此，根据《儿童在线隐私保护法案》，父母仍对其子女的信息享有特定权利。此外，如果以欺诈方式使用某人的个人信息，该个人可向该等滥用或泄露数据的个人或实体

索赔。该等欺诈行为人还可能会受到刑事处罚。

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？

联邦层面或州层面的法律对雇员的个人信息总体不会区别对待。尽管如此，雇主不得基于收集的或向雇主开放的信息（例如个人的医疗史、家庭状态、种族或宗教信仰）进行歧视性的雇佣活动。如发生此类事件，被拒绝雇佣的个人可对雇主提起诉讼。此外，如前所述，在如何披露或分享个人信息方面，对待金融和健康信息与一般个人信息存在区别。

9. 在您所在的法域，什么个监管机构负责实施和执行个人信息保护法律？

FTC、DHS（涉及HIPAA法规）和CFPB是美国负责执行个人信息保护法律的主要联邦机构。此外，各类州层面的机构负责实施和执行州层面关于个人信息的法律法规。

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？

违反关于个人信息的法律法规的，可能会受到政府机构的罚款，被信息受到滥用的个人提起民事诉讼，并承担仅与信息泄露相关的责任。FTC作出的执行行为产生的处罚例如，LifeLock（提供身份保护服务的公司，颇具讽刺意味）同意因未能保护消费者的个人信息而支付1亿美元。导致大规模罚款的原因是LifeLock违反要求其执行该等实践的先前的法院命令且未能保存其努力保护的消费者数据的记录。至于数据泄露如何能导致超出因泄露行为本身导致损害的责任，例如证券交易委员会(SEC)近期因雅虎未能向投资者披露涉及未经授权访问数百万用户账户，包括用户名、电子邮箱地址、密码、出生日期、电话号码以及安全问题答案的数据泄露而对其处以3500万美元罚款。考虑到泄露行为的范围，SEC认为雅虎误导投资者，因为入侵行为很可能具有重大金融和法律影响。

11. 您所在的法域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您所在的法域预计会如何发展？

作为对最近涉及的未经授权披露个人信息的违法行为，美国国会已提出立法议案赋予个人对其个人信息更大的控制权。例如，2018年《社交媒体隐私保护和消费者权利法案》要求网站运营者向用户提供其已被收集信息的副本。根据提出的立法议案，网站运营者还需要提供信息如何被网站使用的详情，说明信息是否已被第三方获取，并在用户数据以任何方式被滥用后72小时内通知该用户。

类似的，加利福尼亚州最近制定了《加利福尼亚州消费者隐私法案》，要求网站向用户展示其被收集的数据，这些数据将如何被使用，并识别能够访问这些数据的第三方的身份。这部法律直到2020年才会生效，已经受到许多技术公司的批判，因此这部数据隐私法律可能会在实施前被修改。

结论

如上所述，美国国会已经提出立法议案保护被网站运营者收集的用户信息。该立法是目前众多被予以考虑的立法之一。另外，由特定机构执行的不需要议会额外授权的美国法规继续随数据类型和使用性质的变化而不断发展。即便法规没有发展，FTC和其他机构作出的执行行动将继续协助定义现

行法律法规项下被认定为“不法”的行为。由于被分割的执行责任、缺乏统一性以及不断变化的立法和执行情况，在美国营业的网站运营者将获益于保护个人信息的各现行标准的并行状态。

作者：Michael Monyok

本指南由Meritas联盟成员律师事务所撰写

Meritas是一个由超过180家提供全方位法律服务的律师事务所组成的联盟，服务于超过240个市场。这些律师事务所均具有严格的服务水准、独立运作并相互合作。与Meritas联盟成员律师事务所联系，您将享受具有当地视角、当地费率的世界一流服务。

访问www.meritas.org ，您可通过律师技能与经验搜索数据库直接了解Meritas联盟成员律师事务所。

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