汇衡律师事务所
HHP ATTORNEYS-AT-LAW

个人信息保护全球指南

第二版

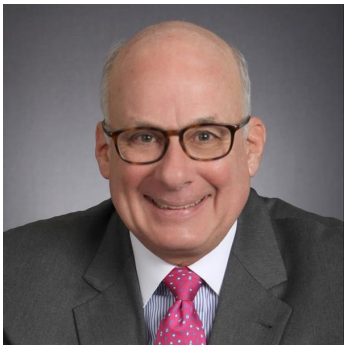
美国

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。

MERITAS®
LAW FIRMS WORLDWIDE

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。

7, 500+
经验丰富的律师

90+
国家和地区

180+
律师事务所

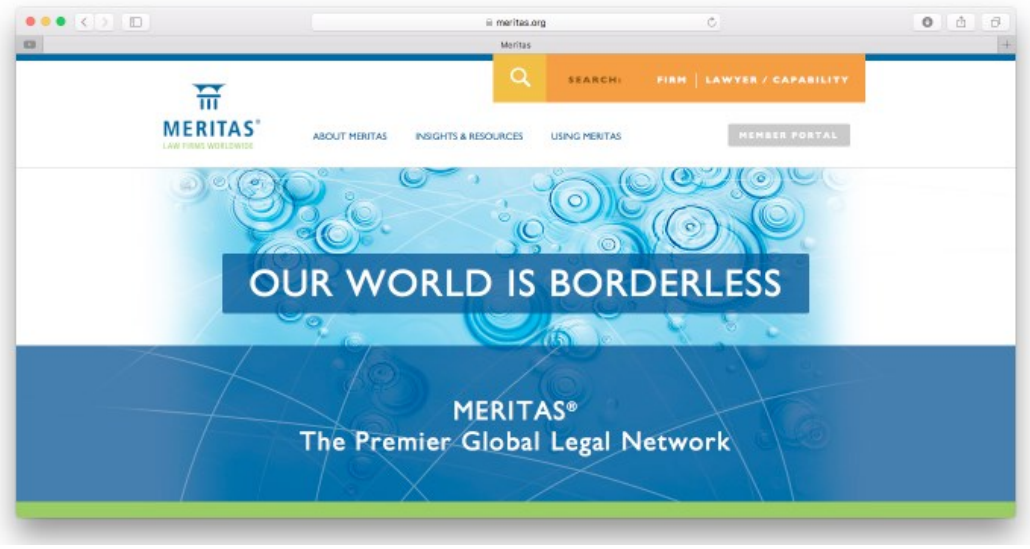
240+
全球市场

MERITAS®
LAW FIRMS WORLDWIDE

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

MERITAS®
LAW FIRMS WORLDWIDE

美国

以下律所可以提供帮助,满足您在美国的数据保护需求。

加利福尼亚

Procopio 律师事务所
San Diego, CA
www.procopio.com

佛罗里达

Smith Hulsey & Busey 律师事务所
Jacksonville, FL
www.smithhulsey.com

Lowndes, Drosdick, Doster, Kantor & Reed, P.A. 律师事务所
Orlando, FL
www.lowndes-law.com

乔治亚

Parker, Hudson, Rainer&Dobbs LLP 律师事务所
Atlanta, GA
www.phrd.com

爱荷华

Nyemaster Goode Des 律师事务所
Moines, IA
www.nyemaster.com

伊利诺伊

Goldberg Kohn 律师事务所
Chicago, IL
www.goldbergkohn.com

印第安纳

Kahn, Dees, Donovan &Kahn, LLP 律师事务所
Evansville, IN
www.KDDK.com

Krieg DeVault LLP 律师事务所
Indianapolis, IN
www.kriegdevault.com

马里兰

Tydings & Rosenberg LLP 律师事务所
Baltimore, MD
www.tydingslaw.com

密歇根

Miller Johnson 律师事务所
Grand Rapids, MI
www.millerjohnson.com

北卡罗来纳

Johnston, Allison & Hord, P.A. 律师事务所
Charlotte, NC
www.jahlaw.com

Wyrick Robbins Yates &Ponton LLP 律师事务所
Raleigh, NC
www.wyrick.com

美国

以下律所可以提供帮助,满足您在美国的数据保护需求。

新泽西

Norris McLaughlin, P.A. 律师事务所
Bridgewater, NJ
www.norrismclaughlin.com

纽约

Carter Ledyard & Milburn LLP 律师事务所
New York, NY
www.clm.com

宾夕法尼亚

Stradley Ronon Stevens & Young LLP 律师事务所
Philadelphia, PA
www.stradley.com

Meyer, Unkovic & Scott LLP 律师事务所
Pittsburgh, PA
www.muslaw.com

田纳西

Chambliss, Bahner & Stophel, P.C. 律师事务所
Chattanooga, TN
www.chamblisslaw.com

德克萨斯

Langley & Banack, Incorporated 律师事务所
San Antonio, TX
www.langleybanack.com

威斯康星

Boardman & Clark LLP 律师事务所
Madison, WI
www.boardmanclark.com

西弗吉尼亚

Kay Casto & Chaney PLLC 律师事务所
Morgantown, WV
www.kaycasto.com

美国

联系人

DENNIS UNKOVIC

du@muslaw.com

MICHAEL G. MONYOK

mgm@muslaw.com

+1-011-412-456-2800

www.muslaw.com

Meyer, Unkovic & Scott LLP. 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，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 LLP就一直是Meritas®活跃成员。

导言

在美国，数据保护是一个至关重要且持续变化的问题。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. 美国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：

（1）《联邦贸易委员会法案》（《美国法典》第15卷第41-58节）：赋予了FTC管理欺诈性和不公平贸易活动的一般权限。FTC将其解释为包含监管网络安全活动和未经授权披露个人信息行为的权限。在FTC对温德姆酒店（Wyndham Hotels）提起的执行程序中，联邦法院确认了FTC的权限。FTC认为温德姆酒店因未能实施合理的安全程序，在三次独立的违规行为中将数十万顾客的支付卡信息不正当地泄露给黑客，进而提起了执行程序。为了解决这一诉讼，温德姆酒店支付了高昂的罚金。

（2）HIPAA法规（《联邦法规汇编》第45篇第160节）：该法规对于医院、医疗保健提供方、医生、医疗保健信息机构和他们的任何商业伙伴收集和使用受保护的健康信息进行监管。

（3）《儿童在线隐私保护规则》（《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。根据这一规则，父母有权控制关于其子女的何种信息可被收集。

（4）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，金融机构需要告知客户其隐私政策和实践做法。此外，该规则还描述了金融机构可能会向非关联第三方披露客户非公开个人信息的情形。

（5）客户信息保护标准（《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、实施并维护一个综合信息安全计划，其应由一个或多个易于访问的部分编写，并包含管理、技术和物理保护”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。

（6）《反垃圾邮件规则》（《联邦法规汇编》第16篇第316节FTC法规）：规范了电子邮箱地址的收集和使用。

（7）《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）：这些法律限制截取传输中或存储中的电子数据以及禁止未经授权的计算机访问。

（8）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漏洞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特定法律或法规的不同而有所差异。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将一个人的姓名、地址、社会安全号码、信用卡号码、账户信息和其他类似数据视为 “个人身份信息”。许多州采用这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存储的任何“个人的可识别健康信息”，无论是电子的、纸质的或口头形式。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可能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（而非法人）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主要原则是：（1）制定并遵守收集和使用客户信息的隐私政策；（2）使用合理保护措施保护个人或敏感信息；及（3）向

所有信息遭到泄露的个人发送违规通知。

尽管“合理”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正当行为时使用的合理”标准相符合，亦满足了HIPAA的要求。例如在FTC的一次执法行动中，FTC主张一家大型国内零售连锁店Petco Animal Supplies未能实施保护消费者信息的政策和程序。如果该连锁店按框架的建议，建立一项组织信息安全政策本可以解决这一问题。

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做法并为客户提供选择退出的权利。

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财务信息外，处理、使用和披露个人信息并不被禁止。就健康和财务信息而言，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建立合同关系，约定接收方同意遵守与披露方相同的安全要求。

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因允许英国的咨询公司访问数百万美国Facebook用户的资料而接受FTC的调查。Facebook的行为还使其受到纽约州和马萨诸塞州检察官的调查。

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？

个人对其信息没有具体特定的权利。并且，由于保留信息不需要取得其同意，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一定的权利。此外，如果个人信息被以欺诈方式使用，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通常不会区别对待。尽管如此，雇主不得基于收集到的或向雇主提供的信息（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，对于财务和健康信息的披露或分享，与一般个人信息有所区别。

9. 在美国，什么监管机构负责实施和执行个人信息保护法律?

联邦贸易委员会（FTC）、卫生与公众服务部（DHS，涉及HIPAA法规）和消费者金融保护局（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，各州级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，以及承担仅与信息泄露相关的责任。举一个FTC执法行为产生处罚的例子，LifeLock（颇具讽刺意味的是这是一家提供身份保护服务的公司）同意因未能保护消费者的个人信息而支付1亿美元。导致其高额罚款的原因是LifeLock违反了先前要求其执行此类实践的法院命令且未能保存其尽力保护消费者数据的记录。

另举一个例子说明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，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亿用户账户的数据泄露，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，而对其处以3500万美元罚款。考虑到泄露的严重程度，SEC认为雅虎误导投资者，因为这样的数据泄露可能会带来财务和法律的重大影响。

11. 美国最近在数据隐私/数据保护方面是否有显著的发展？是否有您认为未来可能影响数据隐私/数据保护的情况？例如，美国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美国预计会如何发展？

针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。根据立法议案，网站运营者还需要提供网站如何使用数据的详情，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。

与此相似，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。这部法律在2020年生效前已经受到许多技术公司的批判，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，美国法规由特定机构执行而不需要国会额外授权，随数据类型和使用性质的变化美国法规也在不断发展。即便法规没有发展，FTC和其他机构的执法行动将继续协助界定现行法律法规项下被认定为非法”的行为。由于执法责任分散、缺乏统一以及不断变化的立法和执法环境，在美国开展业务的运营者如能跟上保护个人信息的各现行标准将有所获益。

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