汇衡律师事务所
HHP ATTORNEYS-AT-LAW

个人信息保护全球指南

第二版

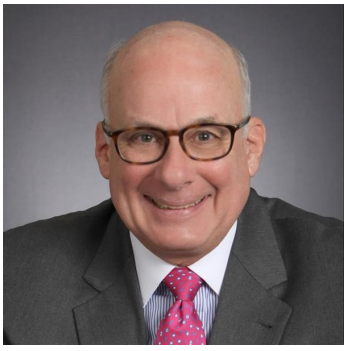
欧洲

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

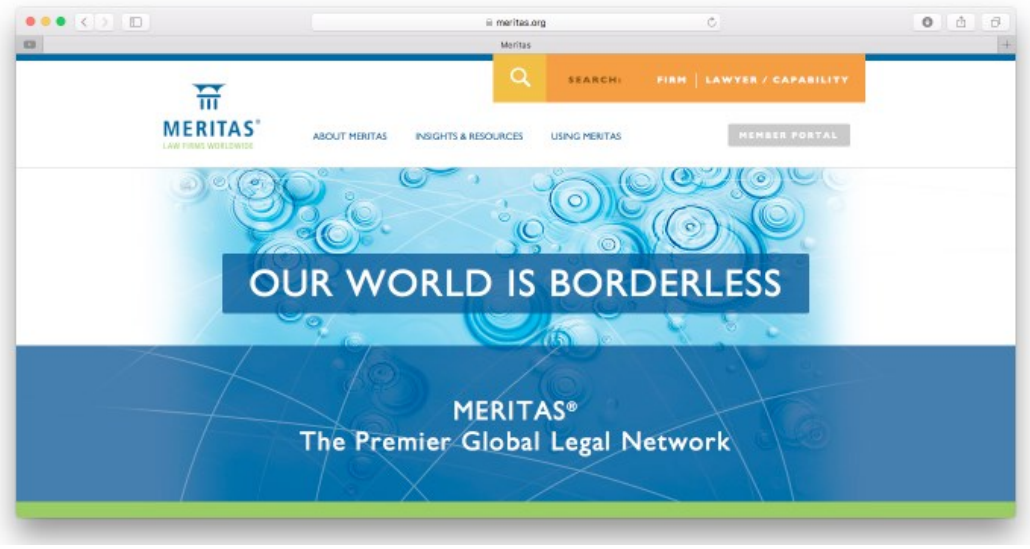
240+
全球市场

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

欧洲

Meritas欧洲数据保护小组是一个协作的成员领导小组，汇集了来自Meritas欧洲网络中的数据保护和隐私法律师。通过合作，小组成员律所能够解决其客户的国内和国际数据保护法律需求；分享对国际监管发展的见解，并提升数据保护法的实务水平。

Meritas成员所就广泛的国内和国际数据保护和数据隐私问题提供法律服务，包括：

- 准备数据保护政策、程序和协议
- 进行数据保护评估和审计
- 就跨境传输个人信息提供法律意见
- 管理与劳动和人事管理相关的隐私问题
- 管理与营销活动和使用客户数据相关的隐私问题
- 确保遵守数据保护法规，包括欧盟GDPR
- 就大数据和数据科学项目提供建议
- 向数据保护专员提供咨询和培训

欧洲

请联系集团的任何成员，以获得特定国家/地区和欧洲数据保护需求的帮助。

奥地利
Siemer-Siegl-Fureder & Partner
律师事务所
Barbara Spanberge
spanberger@ssfp-law.at
www.ssfp-law.at

比利时
Lydian 律师事务所
Bastiaan Bruyndonckx
bastiaan.bruyndonckx@lydian.be
www.lydian.be

保加利亚
Dimitrov, Petrov & Co. Law Firm
律师事务所
Desislava Krusteva
desislava.krusteva@dpc.bg
www.dpc.bg

丹麦
Brinkmann Kronborg Henriksen
律师事务所
Morten Bordrup
mb@bkhlaw.dk
www.bkhlaw.dk

德国
Arnecke Sibeth Dabelstein
律师事务所
Hans Helwig
h.helwig@asd-law.com
www.asd-law.com

爱尔兰
Whitney Moore Solicitors 律师事务所
Emma Richmond
emma.richmond@whitneymoore.ie
www.whitneymoore.ie

意大利
Pirola Pennuto Zei & Associati
律师事务所
Mario Valentini
mario.valentini@studiopirola.com
www.pirolapennutozei.it

卢森堡公国
LG Avocats律师事务所
Hervé Wolff
hw@lgavocats.lu
www.lgavocats.lu

欧洲

请联系集团的任何成员，以获得特定国家/地区和欧洲数据保护需求的帮助。

英格兰和威尔士

Howard Kennedy律师事务所

Robert Lands

robert.lands@howardkennedy.com

www.howardkennedy.com

爱沙尼亚

LEXTAL律师事务所

Rauno Kinkar

rauno.kinkar@lextal.ee

www.lextal.ee

芬兰

Lexia律师事务所

Markus Myhrberg

markus.myhrberg@lexia.fi

www.lexia.fi

法国

Bignon Lebray律师事务所

Elise Dufour

edufour@bignonlebray.com

www.bignonlebray.com

波兰

Domański Zakrzewski Palinka

律师事务所

Bartosz Marcinkowski

bartosz.marcinkowski@dzp.pl

www.dzp.pl

葡萄牙

FCB Sociedade de Advogados

律师事务所

Margarida Roda Santos

mrs@fcblegal.com

www.fcblegal.com

斯洛伐克

BEATOW PARTNERS律师事务所

Miroslava Benediková

miroslava.benedikova@beatow.com

www.beatow.com

瑞士

Wenger & Vieli律师事务所

Claudia Keller

c.keller@wengervieli.ch

www.wengervieli.ch

导言

2018年5月25日，欧盟《一般数据保护条例》（GDPR）生效。作为一项对所有欧盟成员国具有直接约束力的立法，GDPR是一次真正意义的制度变革。过去，尽管确实有成文的法规保护数据主体的权利，但却无法阻止违法行为，因为罚金对于跨国企业而言微不足道。现如今，任何侵权行为将会使企业付出高达其全球营业额4%或高达2000万欧元的代价。现在，个人数据保护必须被严肃对待。

作为一项欧盟条例，GDPR直接适用于各欧盟成员国并对其产生直接效力，替代与之相矛盾的国内法律。尽管如此，GDPR仍允许成员国在一些方面实施比GDPR更为严格的单独的国内规定。

以下是基于我们经常被咨询的有关新规的11个问题制作的一般性概述，也介绍了欧洲不同国家或地区实施GDPR方式的重大改变，以及对不遵守GDPR的公司予以处罚的例子。

1. 欧洲主要的个人信息保护法律或法规有哪些?

2016年4月27日欧洲议会和理事会制定了第2016/679号（欧盟）条例（欧盟《一般数据保护条例》–GDPR），以保护自然人的个人数据处理和此类数据的自由流动。

GDPR代替了《欧共体第95/46号数据保护指令》，旨在统一全欧洲的数据隐私法律，保护并授予所有欧盟公民数据隐私权，重塑跨区域组织机构对待数据隐私的方式。其核心影响为：

（1）GDPR扩大了管辖范围，其适用于所有处理欧盟居民个人数据的公司，而不论该公司位于何处；

（2）严苛的处罚（如上所述）；

（3）就数据主体出具有效同意设置更为严格的条件；

（4）数据主体的扩展权利—包括被遗忘权、数据转移权；

（5）要求企业设置符合法定要求的数据保护专员；

（6）对数据控制者和处理者增加了合规义务；

（7）要求数据控制者证明其合规性的义务。

2. 个人信息是如何定义的?

第4条第（1）款：“个人数据”系指与被识别的或可识别的自然人（“数据主体”）相关的任何信息。

可识别的自然人系指可通过某一识别标记（例如姓名、身份识别号码、位置数据、网络识别码）或其一个或多个物理、生理、基因、心理、经济、文化或社会特征因素而被直接或间接识别的个人。

定义中不包括关于法人或公司的信息，仅限于个人的个人信息，但包括可识别法人成员的信息。死者的个人数据不受到GDPR的保护（序言第27段）。但是，成员国可以就该等数据及其在个人逝世后的后续保护进行规定。

3. 有关个人信息保护的关键原则有哪些?

GDPR第三章：可以收集涉及个人的数据，但前提是其已被告知该等行为。

第5条：个人数据处理应当：

（1）以合法、公平、并且透明的方式对数据主体的个人数据进行处理；

（2）以具体、明确、合法目的收集，并不得以与该等目的不相符的方式进一步处理；

（3）是充分的、相关的，且限制在个人数据处理目的的必要范围内；

（4）是准确的，并在必要时保持更新；

（5）对于以可识别数据主体的形式进行保存的个人数据，其保存期限不长于为个人数据处理目的所必要的期限；

（6）以确保个人数据得到适当保护的方式进行处理。

序言第39段关于存储时间的规定为：“个人数据的

存储期限应严格地限制为最小值。只有在处理目的无法通过其他合理方式实现的情况下才能处理个人数据。为了确保个人数据的保存不长于必要时限，应当由控制者建立删除或定期查看的时间限制。应当采取合理措施确保不准确的个人数据被修正或删除。”

4. 收集个人信息的合规要求有哪些?

GDPR第6条：只有在符合下列至少一项条件时，处理行为才合法：

（1）数据主体已同意基于一个或多个特定目的处理其个人数据；

（2）处理行为对于履行数据主体作为一方的合同而言是必要的，或者进行处理是为了完成数据主体所要求的签约前步骤；

（3）处理行为对于数据控制者履行其法律义务而言是必要的；

（4）处理行为对于保护数据主体或其他自然人的重要利益而言是必要的；

（5）处理行为对于执行涉及公共利益的任务或行使赋予控制方的公权力而言是必要的；

（6）处理行为对于实现控制方或第三方所追求的合法利益目的而言是必要的，除非数据主体的基本权利和自由优先于该等利益，从而需要保护个人数据，尤其是在数据主体是儿童的情形下。

GDPR第13条和第14条：

应在收集数据时通知数据主体，或者，如果个人数据尚未从数据主体处获取，则应在获取个人数据后的合理期限内通知数据主体，但最迟应在一个月内通知以下信息：

（1）数据控制者的身份和数据保护专员的联系方式（如适用）；

（2）收集数据的目的；

（3）在适用的情况下，控制者追求的合法利益；

（4）在适用的情况下，存在自动决策，包括用户画像；

（5）数据的接收者或数据接收者的类别；

（6）数据主体依法享有的权利；

（7）在适当情况下，向非欧盟成员国转移个人数据；

（8）所处理数据类别的保留期；

（9）尚未从数据主体处获取个人数据的，通知个人数据的来源，以及如果适用的话，个人数据是否来自可公开获取的来源。

5. 处理、使用和披露个人信息的合规要求有哪些？

除了对Q4的答复中列出的要素外，个人信息的处理、使用和披露还应包括：

（1）问责制；

（2）提供默认保护和数据系统保护的义务；

（3）在适用的情况下，进行数据保护影响评估的义务；

（4）保存处理记录的义务；

（5）在适用的情况下任命数据保护专员的义务。

如果存在法律依据，即数据主体的同意或遵守法律/监管义务的必要性，则可以披露个人数据。

6. 是否存在转移个人信息至其他法域的限制?

GDPR第44至50条。如果没有采取以下保障措施，则不可以在欧盟/欧洲经济区以外进行转移：

（1）标准欧盟协议（数据控制者至数据控制者以及数据控制者至数据处理者）；

（2）有约束力的公司规定；

（3）向可提供充分保护的国家转移或披露：安道尔、阿根廷、加拿大（仅限商业组织）、法罗群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、瑞士、乌拉圭和美国（在《欧盟-美国隐私护盾》有效期间，接收方符合时）。与韩国正在进行充分谈判。

如果控制者未能采取充分有效的数据保护措施，其应当根据GDPR第82条对数据主体承担责任。另外，根据GDPR第83条第5款规定，GDPR第44至49条规定的侵权行为将被处以不超过2000万欧元或年营业额4%的行政罚款。

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？

GDPR第三章第12至23条规定了数据主体的权利：

（1）信息、交流、以及数据主体权利行使模式的透明性；

（2）个人数据的披露和访问；

（3）从数据主体处收集个人数据以及尚未从数据主体处获得个人数据的情况下，应当被提供的信息；

（4）限制处理权、数据转移权、数据主体访问权、修正权、删除权（被遗忘权）；

（5）关于修正或删除个人数据或限制处理信息转移数据控制者有通知义务；

（6）反对权和反对自动个人决策权。

根据GDPR第7条第3款，数据主体应当有权随时撤回同意；对此，在撤回同意之前基于同意的处理行为的合法性不受影响。撤回行为仅影响根据GDPR第6条(1)(a)基于同意的数据处理行为的合法性。

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？

成员国可以通过法律或集体协议的方式规定更为具体的规则以保护劳动关系情境下处理雇员个人数据的权利和自由（GDPR第88条）。

9. 在欧盟，什么监管机构负责实施和执行个人信息保护法律？

欧洲数据保护监管局（EDPB）是一个独立的监管机构，其主要目标是确保欧洲的机构和团体在处理个人数据和制定新政策时尊重隐私权和数据保护权。

通信地址：Rue Wiertz 60, B-1047 Brussels

办公地址：Rue Montoyer 30, B-1000 Brussels

电子邮箱：edpb@edps.europa.eu

网址：www.edpb.europa.eu

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？

GDPR第83条规定了处罚，根据违法行为处以不超过1000万或2000万欧元或全球营业额的2%至4%的罚款。个人也有权获得民事损害赔偿，并且可以提起集体诉讼要求赔偿损失。

11. 欧盟最近在数据隐私/数据保护方面是否有显著的发展？例如，欧盟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？

欧盟的数据保护影响着每个企业和组织，是不容忽视的重要问题。未来几年，整个欧盟的数据保护和执行法规的范围可能会扩大。

《电子隐私条例》（The ePrivacy Regulation）原定于2018年5月25日与GDPR同时生效，然而，对其一些细节的持续审议和游说推迟了它的颁布。欧盟进一步发布了新的《电子隐私条例（草案）》，仍在讨论修订中。

当然，可以预见的是，整个欧洲与违反GDPR有关的案件将会增加，因为巨额罚款将使得控制者对被处罚采取法律行动。

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