



个人信息保护 全球指南

欧洲

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,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

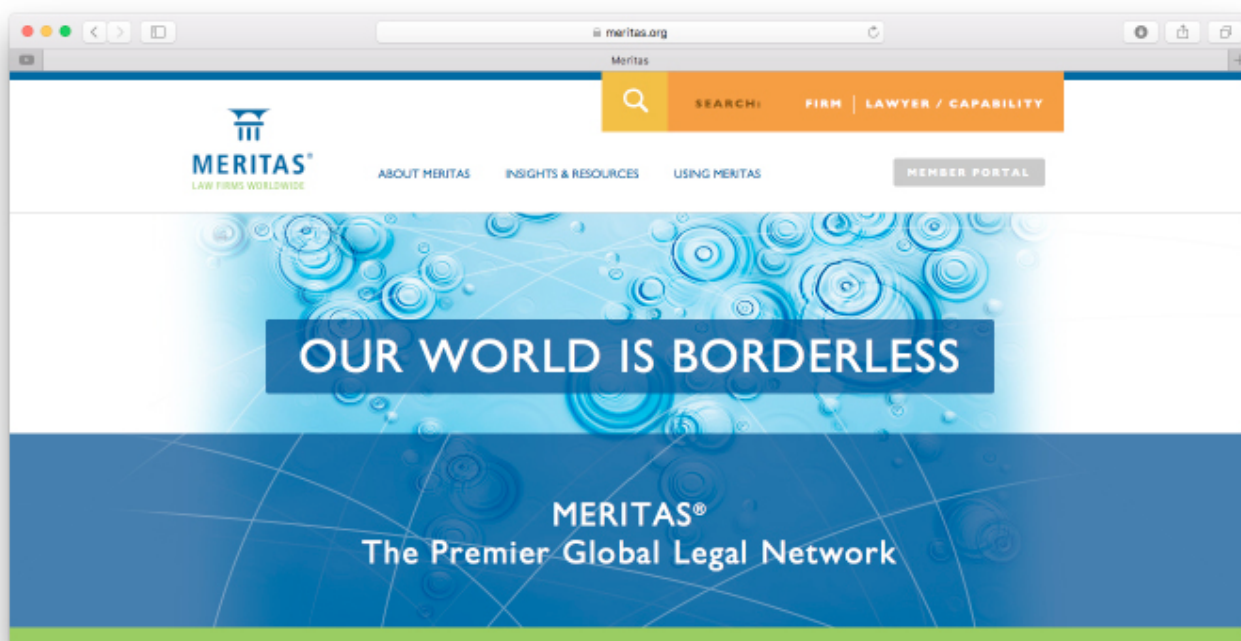
90+
国家和地区

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：



德国 欧洲

律师事务所简介:



ARNECKE SIBETH

DABELSTEIN律师事务所是一家商事律师事务所，涉及12个专业领域，广受关注、值得信赖、品质卓越！作为一家具有领先水平的商事律师事务所，我们凭借在不动产、海事行业以及运输/航空/物流市场领域的核心竞争力受到国际上的认可。

ARNECKE SIBETH

DABELSTEIN律师事务所基于12个突出专业领域，提供全方位的法律建议。我们的专业能力与专业内竞争者难分伯仲，并会在未来不断进步。我们计划在保险、能源和体育/媒体/娱乐领域谋求战略性发展，使其亦成为我们的核心竞争力。

ARNECKE SIBETH

DABELSTEIN律师事务所富有创新精神、充满活力、极具现代化。数十年以来，作为最顶尖的可靠顾问，我们的价值与成功是有目共睹的。

我们的国际网络具有多层结构并且紧密结合。我们作为**Meritas**的成员，是我们国际客户值得信赖的合作伙伴。

联系人:

HANS GEORG HELWIG
h.helwig@asd-law.com

+49 30 8145913-42
www.asd-law.com

法国 欧洲

律师事务所简介:



Bignon Lebray律师事务所成立于1982年，主攻公司法各领域的业务。

我们律师事务所聚集了超过一百位法律专业人士，包括专攻11个实务领域的25位合伙人。

我们文化上和专业上的多样性反映了我们的历史：我们是一家随客户在如今全球化商业世界中的发展而不断成长的独立法国律师事务所。

我们为各类公司提供服务，从初创企业到上市公司。我们也为公共机构和非营利组织提供服务。对我们客户商业活动和项目的透彻理解，正是我们在各类法律和诉讼事务中所关注的法律焦点。

通过我们在法国（巴黎、里昂、里尔和埃克斯-马赛）的4家办事处和在中国（上海和北京）的两家办事处，我们努力针对客户的商业需要为客户带来最高效、最具性价比、与具体情况最相契合的答案。

联系人:

ÉLISE DUFOUR
edufour@bignonlebray.com

+33 (0)1 44 17 17 44
www.bignonlebray.com

导言

2018年5月25日，欧盟

《一般数据保护条例》

（GDPR）生效。作为一项直接对所有欧盟成员国具有约束力的立法，GDPR是一次真正意义的范式转移。过去，尽管成文规定确实保护数据主体的权利，但却无法阻挡违法行为，因为罚金对于跨国企业而言轻如鸿毛。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2000万欧元的成本。现在，个人数据保护必须被严肃对待。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要，也提供了德国法和法国法将如何在相应国家适用GDPR的一些参考。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在一些方面仍允许成员国实施比GDPR更为严格的单独国内规定。

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？



2016年4月27日欧洲议会与欧盟理事会关于保护自然人数据处理与自由转移同时

废除欧共体第95/46号指令的第2016/679号（欧盟）条例（《一般数据保护条例》——GDPR）

欧盟《一般数据保护条例（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) 扩大了GDPR的管辖范围，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) 被遗忘权、数据转移权；
- (5) 由企业聘任法定要求的数据保护官。



1978年1月6日关于信息技术、数据文档和民事自由的第78-17号法案

尽管条例可以直接适用，但其已经于2018年6月20日被并入国内法律。



2018年《联邦数据保护法》（缩写：BDSG），用以实施GDPR。

在GDPR允许的情形下，BDSG制定了更为严格的规则。

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特别通过某一识别标记（例如姓名、身份识别号码、位置数据、网络标识符）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，但包括可识别法人组成人员的信息。

已故人员的个人数据不受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。



根据前述法律第2条的规定，适用与GDPR一样的定义。



BDSG援引GDPR第4条，因此未予规定更具体的定

义。但是，根据德国的判例法，个人的商业电子邮箱地址被视为“个人数据”。

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13条）

第5条：个人数据应当：

(1) 合法地、公平地并以对数据主体而言透明的方式被处理（“合法性、公平性和透明性”）；

(2) 为具体、明确、合法的目的被收集，并不得以不符合这些目的的方式被进一步处理（…）；

(3) 就个人数据处理目的而言，是充分的、相关的，且限制在必要范围内（“数据最小化”）；

(4) 是准确的，并在必要时保持更新（…）（“准确性”）；

(5) 以可识别数据主体的形式进行保存的期限不长于为个人数据处理目的所必要的期限；（…）（“存储限制”）；

(6) 以确保个人数据得到适当保护的方式进行处理（“完整性”）。

序言第39段关于存储时间的规定为：“尤其要确保个人

数据的存储期限绝对最短。只有在处理目的无法合理通过其他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，应当由控制方建立删除或定期查看的时间限制。应当采取每一合理步骤确保不准确的个人数据被修正或删除。”



根据前述法律第6条，规定了相同权利。



BDSG援引GDPR并因此规定了相同权利。

4. 收集个人信息的合规要求有哪些？



GDPR第6条：只有在符合至少下列条件之一时，处理行为才合法：

(1) 数据主体已同意为一个或多个特定目的处理其个人数据 [根据第7条和序言第32段 – 同意不是必须以书面形式作出；而控制方应当要求书面同意以便能够证明同意已经作出，GDPR第7条第1款]；

(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) 处理行为对于遵守控制方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：数据主体应当被立即告知：

(1) 数据控制方的身份；

(2) 目的；

(3) 是否必须答复；

(4) 对其而言不回应的可能后果；

(5) 接收人或数据接收人的类型；

(6) 根据法律数据主体拥有的权利；

(7) 适当情形下，个人数据向欧共同体成员国以外的转移；

(8) 被处理的不同类型数据的保留期限。



根据前述法律第32条，规定了相同的要求。



德国《联邦数据保护法》第32至37条规定了相同的机制。

5. 处理、使用和披露个人信息的合规要求有哪些？



见问题4的回答。

对个人数据的披露只有在数据主体同意的情形下才可接受。



根据前述法律第34条，数据控制方应当考虑数据的性质和处理行为带来的风险从而采取所有合适的预防措施，以此保护数据的安全性，尤其是防止其被曲解、损坏或被未经授权的第三方访问。



见问题4的回答。

如果个人数据并非从数据主体处获得，而是经由第三方获得，GDPR第14条和BDSG第33条规定了针对控制方的特别知情权，比如：

- (1) 控制方和数据保护官的身份和具体联系方式；
- (2) 处理个人数据的目的和法律依据；
- (3) 涉及数据的类型；
- (4) 数据接收方；
- (5) 确保公平和透明处理，

包括：

- 存储期限
- GDPR第5条规定的权利
- 向监督部门提出投诉的权利
- 个人数据来源

(6) 该等信息必须在获取数据后的合理时间内提供。

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

只有采取如下保障措施后才能转移：

- (1) 标准欧盟协议（数据控制方至数据控制方，与数据控制方至数据处理方）；
- (2) 有约束力的公司规定；
- (3) 向可提供充分程度的保护的国家转移或披露。

如果控制方未能采取充分程度的数据保护措施，其应当根据GDPR第82条由其自身向数据主体承担责任。另外，根据GDPR第83条第5款规定，GDPR第44至49条规定的侵权行为应当被处以不超过2000万欧元或年营业额4%的行政罚款。



根据前述法律第69至70条，若非属于欧盟成员国的国家不提供充分程度的个人隐私、自由和基本权利的保

护，数据控制方不得将个人数据转移至该国。存在一些例外情况。



就数据向第三国转移的前提条件，BDSG在第78至81条中进行了非常详尽的规定。

其包括：

(1) 如果数据主体的基本权利不是更值得保护的，将个人数据转移至第三国的执法机构。

(2) 根据（欧盟）指令第2017/680号第36（3款）基于欧盟委员会的充分性决议的转移，即委员会已经决议认为所涉第三国符合欧盟数据保护标准（欧盟委员会会定期更新清单，以列示被认定为“充分”的国家及相应决议）。

(3) 在没有该等决议时，如果第三国出具了具有法律约束力的保证，保证对个人的个人数据提供充分保护，例如美国-欧盟隐私护盾协议，则允许向该国转移。

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12至23条：

(1) 透明的信息、沟通和数

据主体权利的行使方式。

(2) 个人数据的披露和访问。

(3) 从数据主体处收集个人数据的情况下，以及尚未从数据主体处获得个人数据的情况下，有待提供的信息。

(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的通知义务。

(6) 反对权和自动化个人决策。

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。另外，根据GDPR第6(1)(a)条，撤回行为仅影响基于同意的数据处理行为的合法性。



根据前述法律第38、39和40条，规定了相同权利，但法国还有额外规定：根据前述法律第40-1条，数据主体还有权规划其去世后其个人数据的去向。



数据主体的权利规定在BDSG第32条及后续条款，并且与GDPR的标准类似。除GDPR第5条和第6条列出的一般原则（见问题3和4）

之外，一项基本变化是根据GDPR第13条规定了数据主体的知情权，例如，

(1) 控制方的身份和具体联系方式；

(2) 数据保护官的具体联系方式；

(3) 处理个人数据的意图目的以及处理行为的法律依据；

(4) 在基于第6(1)条(f)项进行处理的情况下，控制方或第三方追求的合法利益；

(5) 个人数据接收方或接受方的类型；

(6) 转移至第三国的依据；

(7) 存储期限；

(8) 反对权和删除权的存在；

(9) 在处理行为以同意（GDPR第6(1)条(a)项）为基础的情形下，随时撤回同意的权利；

(10) 向监管机构提出投诉的权利。

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关于雇员个人数据处理的权利和自由（GDPR第88条）



法律没有为雇员的个人信息保护制定特别的框架。但是，根据CNIL的决定，应当征得雇员同意并采取额外的保护措施。甚至，CNIL认为雇员的同意并非自由作出，因此不构成处理雇员数据的有效法律基础。所以，雇主应仅能为劳动合同的签署或其合法利益而收集数据。



BDSG第26条执行GDPR中的规定。

除制定法外，劳动关系中还可以通过集体协商和工会代理协议为数据处理提供依据。

例如，集体协议经常为信息技术的使用制定规则，尤其是互联网和邮件设备。这包括雇员账户的可访问性。未经雇员同意，雇主不得访问雇员的邮箱账户，然而工会代理协议或集体协商协议可以规定雇主即使未获同意也有访问权利。

9. 在您所在的法域，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（EDPS）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和数据保护权。

通信地址: Rue Wiertz

60,B-1047布鲁塞尔

办公地址: Rue Montoyer

30,B-1000布鲁塞尔

电话: +32 2 283 19 00

电子邮箱:

edps@edps.europa.eu

网址:

www.edps.europa.eu



CNIL，即“国家信息自由委员会”，负责在法国实施和执行个人信息保护法律。CNIL的详细信息为: CNIL

3, Place de Fontenoy

75007 巴黎，法国

电话: 01 53 73 22 22



州数据保护专员 – 德国各16个州都有其各自的专员负责。

另外，联邦数据保护专员作为国家监管机构，建立了所谓的单点联系（联络中心 - www.bfdi.bund.de/ZAST/EN）。联邦德国的体系在全欧洲境内独树一帜，其包括联邦政府和各16个州（联邦州）的数据保护监管机构。这种体系下，单一联系点协调与其他欧盟成

员国、欧盟数据保护理事会（EDPB）以及欧盟委员会之间的跨境合作。联络中心由联邦数据保护和信息自由专员建立，但从组织上与该机构相独立。

作为单一联系点，联络中心应当使其他成员国、EDPB和欧盟委员会的监管机构能够与德国监管机构进行有效沟通。

在针对市民、权力机构与公司的外部关系中，其并不活跃。

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，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%的行政罚款。



第45条

CNIL可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%的行政罚款。

另外，特定的违法行为会受到刑法处罚并可被处以五年监禁和300,000欧元罚金（对法人的罚金是其5倍）（刑法典第226-16至226-24条）。



根据BDSG第41条，GDPR第83条可直接适用。

就对于BDSG第30条规定的数据主体的信息权利的侵犯行为，BDSG第43条将罚金进一步限制在最高50,000欧元。

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？



欧盟的数据保护影响到每项业务和每个组织，无法被忽视。

欧盟范围内，数据保护的范范围和实施细则在未来几年将很可能增加。

除GDPR外，电子隐私条例拟在2019年初的前6个月内生效。这一条例更多指向于电子商务的规定，其原本打算在2018年5月25日与GDPR一并生效。

的确，全欧洲都会预测关于违反GDPR的司法案件将会增加，因为高昂的罚金会促使控制方采取诉讼对抗施加的罚金。



针对个人信息保护的一部法律最近已经被通过：2018年

6月20日第2018-493号法律，
该法于2018年6月21日公布，对1978年1月6日的《信息与自由法》进行了修订。
实施该法律的法令已于2018年8月1日被通过。



GDPR已通过BDSG加以实施。电子隐私将随后实施。

结论

欧盟目前由28个国家组成。本概览以法国和德国为例阐述了GDPR中的合规要求和义务如何根据欧盟成员国国内转换法律的差异以及欧盟成员国对GDPR条文的不同解释而在国家与国家之间产生差异。

我们建议您的业务严格遵守GDPR中规定的所有标准。您的义务会比本概览中所涉及的更加广泛。例如应当立即建立您处理活动的记录，履行删除错误信息的义务，并采取技术性和组织性措施。

对GDPR和国内法律要求的违反或不合规将会使您的企业遭受高昂的罚款。另外，这可能还会危及到跨境关系，因为业务伙伴会核查对GDPR所有规定的合规情况。

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。



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