Blackboard 实施 GDPR 对客户的益处

欧盟《通用数据保护条例》(General Data Protection Regulation, GDPR) 是一次重大变革。Blackboard 热烈拥护这一变革。我们重视数据隐私权，也理解它是一项人权。GDPR 进一步加强了个人权利，并将推动数据隐私做法的改进和完善。这样的变革对于个人和组织都是有益的，也将增强个人和组织间的信任。

我们发布本文档旨在向客户简要介绍 GDPR 做出的变更及存在的误解，阐释我们的实施办法，并详细介绍我们的工作将对贵组织产生的帮助。我们重点挑出我们认为对您最有用处的信息。因此，本白皮书绝不是全面的 GDPR 指导。[1]

这些材料仅供提供信息之用，不作为法律建议。关于 GDPR 在贵组织的实施以及相关的法律问题，请向贵组织内部或外部律师咨询建议。

GDPR 引进了一系列重大变更，但在 Blackboard，我们本就已经形成了完善的数据隐私实践（例如，欧盟 - 美国隐私盾认证）。我们将 GDPR 视为进一步改进我们的行为实践的契机。并且我们将继续以客户为中心，协助您实现数据隐私合规。

目录

GDPR – 您需要知道些什么	**3**
为什么颁布一项新法律？	3
有哪些新增规定？	4
哪些规定保持不变？	4
Brexit 产生了什么影响？	5
揭秘 GDPR	**6**
正确对待数据隐私和 GDPR 的重要性	7
我们及贵组织在 GDPR 中的角色	7
您可以为 GDPR 做些什么准备？	7
BLACKBOARD 的实施计划和办法	**9**
Blackboard 的数据隐私和安全	9
Blackboard 的 GDPR 实施办法	10
以 GDPR 为契机	10
我们的实施计划	11
变更概述	12
1 GDPR 就绪产品	13
2 通过设计保护隐私	14
3 数据传输	15
4 和客户订立合同	16
5 管理我们的供应商	16
6 安全	17
管理信息安全风险	17
不止步于 GDPR……	18
安全成熟度评估和路径图	18
结论	**19**
GDPR 实用资源	**19**
欧盟官方资源	19
欧盟数据保护机构材料	19
法律事务所指南	19
其他组织	19
更多信息	**20**
资料来源	21

Blackboard 通过了隐私盾认证，并且荣幸地签署了《学生隐私承诺书》并加入了隐私未来论坛。

GDPR - 您需要知道些什么

GDPR 是新颁布的一项欧盟数据保护条例，将取代原来的欧盟数据保护指令 96/46（“指令”）以及在欧盟成员国实施的数据保护法（例如，1998 年英国《数据保护法》）。

GDPR 在 2016 年 5 月通过，2018 年 5 月 25 日正式实行。

下文简要介绍（极不详尽和全面）了 GDPR 要求。您可以在“GDPR 实用资源”部分找到更多详细指南的链接。

为什么颁布一项新法律？

欧盟的立法机关和执法机关坚信指令需要更新，以解决缺乏协调统一性的问题并适应在实行指令的这 20 年来取得的社会和技术发展。在他们所列出的更新清单中，排在前面的分别是加强执法力度、扩大地域范围和增强个人权利。

新增的许多规定（例如，域外效力）主要针对的是位于欧盟以外的社交媒体和互联网公司。欧盟的立法机关和执法机关认为原来的指令无法对使用此等社交媒体和互联网服务的欧盟公民的数据隐私权利提供充分的保护。

和那些基于用户数据的“资本化”建立经营模式的社交媒体和其他互联网公司相比，Blackboard 采用不同的经营模式。我们在客户的指示下收集和使用客户个人信息[2]，并向他们及其用户提供我们的产品和服务。我们不会为了出售信息或出售广告而收集或使用个人信息。我们理解这些个人信息是委托给我们的，我们为此负有责任。因此，我们和我们的客户有保护此等信息的安全的共同利益和共同责任。

有哪些新增规定？

尽管 GDPR 是以原来的欧盟数据隐私原则和概念为基础，但为欧盟的数据隐私制度带来了显著的改变，包括：

- 将罚款力度提高到全球营业额的 4% 或 2000 万欧元（以较高的金额为准）
- 将地域范围扩大到位于欧盟境外但向欧盟居民提供产品和服务或监视欧盟居民的组织
- 强制要求数据控制者[3]必须在 72 小时内向监管部门发出违规通知
- 有关同意的要求更加严格
- 增加个人权利（包括数据擦除权利和数据迁移权利）

但其中一些最重要的变化是引进了问责制原则和通过设计保护隐私的原则。这些原则要求实施有效的数据隐私管理和流程，并要求就组织如何遵守 GDPR 的要求制定详细完善的文件。

哪些规定保持不变？

GDPR 中的许多概念和定义仍和指令相同或相似：

- “个人数据”（或个人信息）的定义仍大体相同，但现在明确包括 IP 地址、Cookie 和设备标识符
- “数据控制者”和“数据处理者”的概念相同（但 GDPR 对数据处理者规定了更多直接责任）[4]
- 在指令中规定的处理原则（例如，合法公平地处理、目的限制、个人数据仅保留必要期限）仍保留
- 关于数据传输的要求仍大体相同：只要是采用了经核准的数据传输机制（例如，欧盟 - 美国隐私盾或“示范条款”）[5]，就可以将数据传输到欧盟/欧洲经济区以外

GDPR 加大了罚款力度，这意味着如果不遵守现有的原则和要求，例如个人数据仅保留必要期限或实施适当的安全保护措施，所带来的风险将更高。

英国脱欧有什么影响？

从 2018 年 5 月 25 日起直到 2019 年 3 月底“英国脱欧”，GDPR 在英国直接适用。但即使是在英国脱欧后，GDPR 也将确立适用于英国的标准：

- 英国政府发布了 2017 年《英国数据保护法案》（目前正在立法过程中），在英国脱欧[6] 前后实施 GDPR
- 英国脱欧后，GDPR 直接适用于向欧盟居民提供产品和服务或监视欧盟居民的组织（例如，积极招收欧盟学生的英国大学）

对将数据传入/传出英国的影响：

- 欧盟已经明确声明，英国在脱欧后将被视为“第三国”，即不再被视为“提供充分保护”（被列入白名单）的数据传输国家。
- 除非且直到英国被欧盟委员会认定为提供充分保护（例如，作为过渡性交易的一部分），否则从欧盟向英国传输个人信息应订立数据传输协议或采用其他数据传输机制。
- 反之，英国需确定其认为哪些国家/地区提供充分保护（可能包括欧盟国家和被欧盟列入白名单的国家/地区）。对于被视为不能提供充分保护的国家/地区，将个人信息传输到英国以外将需要使用英国认可的数据传输机制（可能和欧盟机制相似）。

揭秘 GDPR

GDPR 的其中一个目标是通过更加详尽的规定进行进一步澄清和明确。但是，GDPR 仍然有许多可进行开放性解读的地方。而且由于 GDPR 的复杂性，导致其未得到充分理解以及各种夸大的说法。这样便产生了许多误解。下面我们就其中的几个误解进行澄清：[7]

误解 1：一切个人信息的处理均需征求同意

事实：同意仅仅是允许处理个人信息的多种法律依据（例如，因履行合同或出于组织的“合法权益”而需要处理）的其中一种。对同意的限制已经变得十分严格。例如，除非个人具有真正意义上的自由选择权，并且可以随时撤回同意且不招致任何不利后果，否则就不被视为是有效的同意。在许多数据处理情况中，其他法律依据将更加合适。[8]

误解 2：72 小时违规通知期适用于整个供应链（即，从处理者/次级处理者知悉违规情况开始）

事实：GDPR 要求数据处理者在知悉个人数据泄露的情况下“无不当延迟”地通知其数据控制者。仅当数据处理者通知控制者后，才开始计算适用于数据控制者的 72 小时通知期。第 29 条“工作组”(WP29)，即欧盟数据保护机构组，在最终指南[9]中明确界定“无不当延迟”是指“及时”通知（不同于上一版本的“立即”通知）。

误解 3：不允许将数据传输至欧盟/欧洲经济区以外，或者必须每次得到客户的同意方可传输

事实：GDPR 大致保留原来的数据传输要求。因此，如果实施了经欧盟核准的诸如欧盟 - 美国隐私盾或经欧盟核准的示范条款（数据传输协议）等数据传输机制，则可进行数据传输。Blackboard 同时实施了两种机制以合规地传输客户的个人信息。[10] Blackboard 充当的是数据处理者的身份，因此需就数据传输征得客户的一般指示（包含在我们的标准数据处理协议中），但不需要在每次传输数据时均征求客户同意。

误解 4：擦除权要求组织删除所有有关个人的数据

事实：新引进的擦除权不是绝对的“被遗忘权”，而是当数据不再需要使用以及在组织未符合 GDPR 要求的其他情况下将数据删除的权利。如果组织仍然合理地需要保留数据（例如，由于记录保留要求），则无需删除该个人信息。

误解 5：GDPR 适用于所有招收欧盟学生的大学。

事实：仅凭招收欧盟学生这一项要求不足以成为适用 GDPR 的条件。GDPR 一般适用于位于欧盟的机构，另外还适用于位于欧盟以外其他国家和地区的大学，但前提是其向欧盟居民提供产品和服务或监视欧盟居民的行为。要被认定为“提供服务”，需满足具备一定程度的目标性的条件。仅凭招收欧盟学生这一点不足以作为充分条件。但如果大学积极以欧盟居民为目标对象（例如，网络课程）或积极招收位于欧盟国家的学生，则可能适用 GDPR。这些条件具备可解读空间。我们建议客户另行咨询法律建议。

实施 GDPR

正确对待数据隐私和 GDPR 的重要性

罚款全球营业额 4% 的风险无疑是许多组织更加重视数据隐私的原因。但我们认为实施良好的数据隐私实践的积极理由至少同样具有说服力，因为数据隐私权是一项人权，且实施良好的数据隐私实践可以建立信任。

在当今社会中，个人信息无处不在。个人信息通常被称为经济中的新石油。我们都会使用网络服务并传递我们的个人信息。但无数研究结果表明，在涉及到个人信息时，组织并没有受到信任。人们普遍认为对自己的数据失去了控制权。立法者和监管机关对此做出了应对。GDPR 可能是最显著的例子。组织需（再次）获得个人的信任。良好的数据隐私实践是建立信任的关键，也是一项竞争优势。最后，它还可以促进组织创新。如果学生（和职员）信任您的组织，就更有可能分享他们的信息并使用新的工具。

破坏数据隐私可能造成毁灭性的打击。数据泄露事件在新闻中常有报道。它导致声誉受损、失去个人信任并带来因滥用数据而遭到索赔的风险。数据保护机构可能不会一开始就判罚营业额的 4%，但他们可以使用许多其他执法手段，还可以强制组织机构改变其数据实践、实施数据隐私计划并定期开展外部审核。

我们及贵组织在 GDPR 中的角色

GDPR 保留了“数据控制者”和“数据处理者”的概念。该概念非常重要，因为其是确定组织及其服务提供者的责任和职责的关键。

如果组织决定处理个人信息的“方式和目的”，即为什么使用个人信息及如何使用个人信息，则该组织被视为数据控制者。另一方面，数据处理者是代表数据控制者并在其指示下开展行动的组织。

就 Blackboard 的大部分产品和服务（例如，Learn、Collaborate、Open LMS）而言，Blackboard 被视为数据处理者，而我们的客户则被视为数据控制者。

GDPR 对如 Blackboard 这样的数据处理者提出了更加直接的要求。但是，GDPR 的大部分要求仍然适用于数据控制者（例如，告知个人其数据将被如何使用的责任、同意个人提出的访问其数据的要求、强制要求将数据泄露事件通知数据保护机构和个人）。

您可以为 GDPR 做些什么准备？

GDPR 所适用的所有组织均需在 2018 年 5 月 25 日前做好准备。以下为客户提供了一些重要的准备建议。其中列出的措施是基于我们的经验而得，内容并不详尽。请务必雇请数据隐私专家协助您实施。许多数据保护机构还制定了关于如何实施 GDPR 的指南。[11]

希望您已经完成了第 1 - 6 步，并且目前已进入实施行动计划的中期阶段。但现在开始也犹未为晚。即使您只是刚刚起步，也可以实施大部分的重要变更。这也意味着您能够向数据保护机构证明您正在实施计划。对 GDPR 置之不顾是不可行的。

1. **检查 GDPR 是否适用于您的组织**

   如果贵组织位于欧盟，则适用 GDPR。但 GDPR 还可能适用于位于欧盟以外的组织。[12]

2. **成立 GDPR 项目**

   设计和实施一个专门的 GDPR 项目。最好在每个部门安排项目管理支持资源和指定联系人，以便对您的工作给予支持。该项目将涉及贵组织的所有部门，并且您会需要得到帮助。

3. **指定一名有经验的 GDPR 负责人管理项目**

   该负责人不仅要有丰富的数据隐私经验，还应有充足的时间和资源，并且能够获得外部支持（例如，律师事务所）。如果贵组织是在欧盟成立的公共机关，您还需指定一名数据保护官。

4. **确保得到高级管理层的支持和监督**

   如果没有高级管理层的支持、指导和监督，GDPR 的实施工作将难以展开。

5. **审查您对个人信息的使用并执行差距分析**

   了解使用个人信息的场合和方式，以及哪些地方需要按照 GDPR 进行改进，是 GDPR 项目的第一个重要阶段。

6. **制定消除差距的行动计划**

   这可能是 GDPR 最困难的部分，因为它要求将往往极为宽泛的 GDPR 要求转化为在各个不同流程和系统中予以执行的具体且切实可行的行动。

7. **实施行动计划**

   信任会有所帮助，但在这种情况下，控制更为有效。这一阶段要求追踪其他人的行动计划，以确保满足进度要求。

8. **审查供应商**

   根据 GDPR，您对供应商承担责任。制定适当的合同规定非常重要，但不充分。您需保证供应商满足 GDPR 要求并且可以支持您满足这些要求。询问他们是如何实施 GDPR 的。

9. **实时掌握法律/法规发展动态（第 29 条工作组指南“成员国实施法律”）**

   知道 GDPR 就够了吗？错！尽管 GDPR 直接适用，但所有欧盟成员国均在各自的国家实行了补充性的数据保护法律。这是为了管控成员国具有立法权限的领域（例如，员工数据隐私）或 GDPR 允许成员国进一步立法的领域（例如，DPO 和 DPIA 条件）。此外，WP29 也将发布重要指南。掌握实时动态具有挑战性，但很重要。[13]

BLACKBOARD 的实施计划和办法

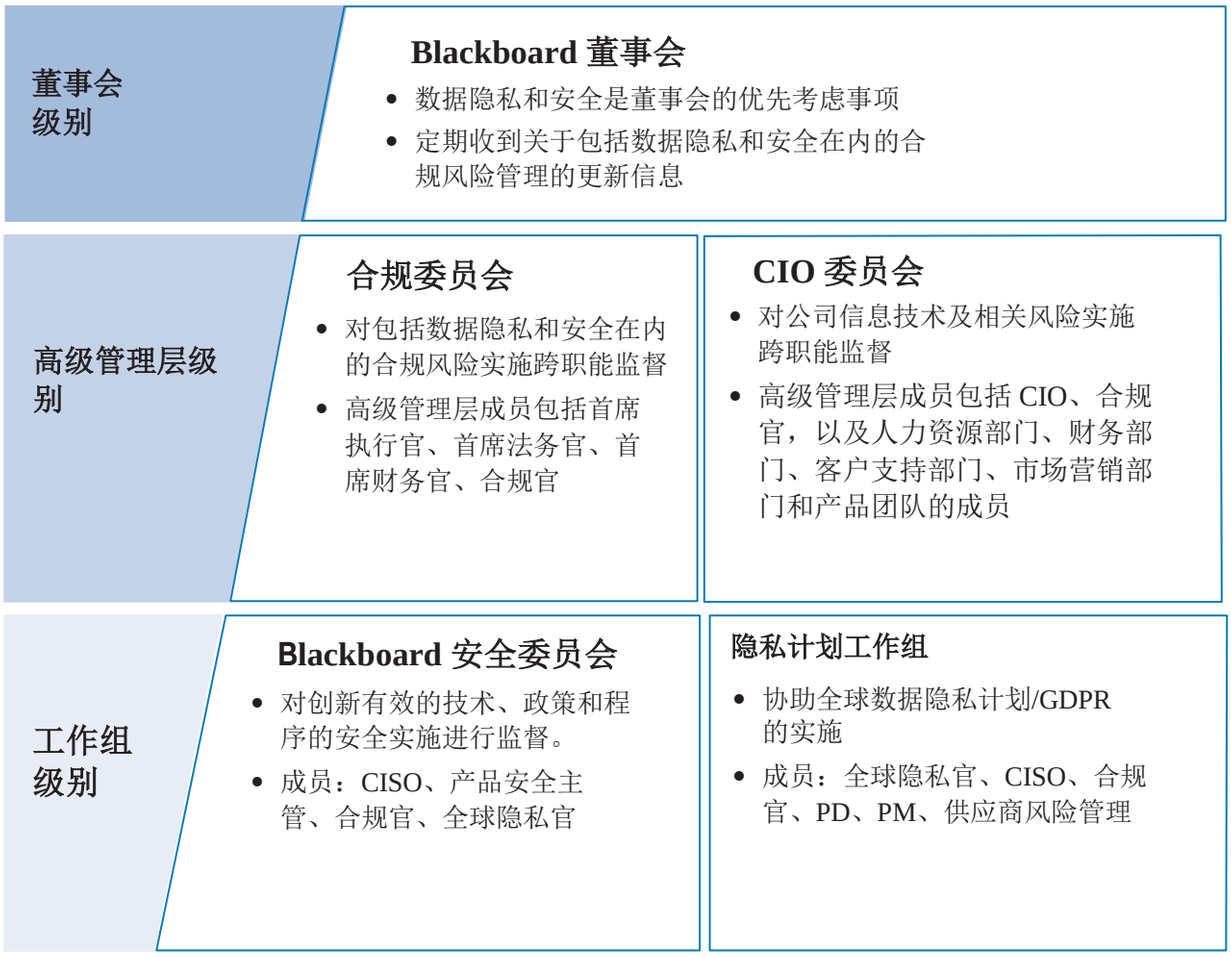
Blackboard 的数据隐私和安全

数据隐私和安全是 Blackboard 一直重点关切的领域。对于我们而言，GDPR 是我们进一步加强当前数据隐私实践的机会。

我们在数据隐私方面的做法一直是以客户为中心。我们了解客户面临的挑战，并希望为他们提供帮助。

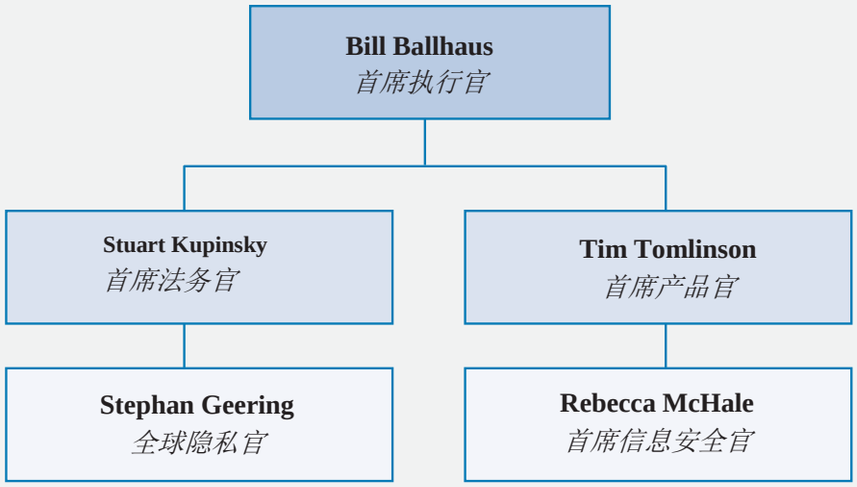
要形成良好的数据隐私实践，需要建立稳固的治理模式。在 Blackboard，数据隐私和安全是 Blackboard 的重要关切领域。我们的治理模式（见下文）确保高级管理层对我们的数据隐私和安全工作进行监督并给予支持。

我们的全球隐私官和首席信息安全官[14]向 CEO 领导层团队报告（见下文的组织结构图），这也突显了 Blackboard 对数据隐私和安全的重视。



隐私和安全

我们的全球隐私官和首席信息安全官向 CEO 领导层团队报告，这也突显了 Blackboard 对数据隐私和安全的重视。



Blackboard 的 GDPR 实施办法

我们成立了一个综合项目，以通过以下办法实施 GDPR 要求：

- GDPR 的实施建立在 Blackboard 已有的数据隐私经验和合规机制上
- GDPR 的实施由全球隐私官领导，由专门的项目经理和各职能单位的“GDPR 负责人”协助
- 包括著名律师事务所 Bristows LLP 在内的多家律师事务所受雇为 GDPR 的实施提供支持
- GDPR 的实施由公司 CEO、首席法务官和其他高级管理人员组成的 Blackboard 合规委员会予以监督

以 GDPR 为契机

我们认为实施 GDPR 不仅仅是为了遵守新的欧盟数据隐私要求，而是一个机遇。我们力求利用实施 GDPR 这一契机来实现以下目标：

- 加强全球数据隐私实践
  - 我们将利用 GDPR 项目在欧盟以及世界其他国家和地区改进我们的全球数据隐私计划
- 制定通过设计保护隐私流程，进一步将数据隐私合规贯彻到我们的日常流程中
- 支持我们的客户开展 GDPR 合规工作
- 将 Blackboard 打造成为教育技术领域公认的数据隐私领导者

我们的实施计划

我们按照 Bristow LLP 确立的三阶段方法实施我们的全球数据隐私/GDPR 计划。该方法已经被包括领先的科技公司在内的许多其他公司采纳。三个重要阶段分别为：

- **第 1 阶段 - 搜集信息**
- **第 2 阶段 - 制定解决方案**
- **第 3 阶段 - 实施工作流**

我们已经运用该三阶段方法制定了一项计划，该计划由以下四个重要环节组成：

项目启动

在项目启动环节中将开展以下活动：

- 高级管理层汇报和支持
- 聘请全球隐私官负责领导 GDPR 项目
- 制定项目计划和项目治理方案
- 初步搜集信息，评估当前合规活动以确定需要根据 GDPR 进行改进的领域

第 1 阶段 - 搜集信息（研讨会）

在初期阶段，我们和来自 Blackboard 职能单位和产品组的重要相关人员开展了有组织有计划的谈话/研讨会，以详细了解这些领域的数据处理做法。

根据研讨会的成果开展差距分析，并制定要在第 2 阶段执行的解决方案和实施计划。

第 2 阶段 - 制定解决方案

我们基于研讨会得到的信息制定了如下解决方案和文件：

- 进一步完善的内部数据隐私文件（政策和详细实施标准），体现了 GDPR 要求并介绍在各种数据处理活动中将如何满足 GDPR 要求（例如，对处理客户数据的要求、通过设计保护隐私过程）
- 产品要求
- 各职能单位实施计划以及关于统一开展工作的实施计划

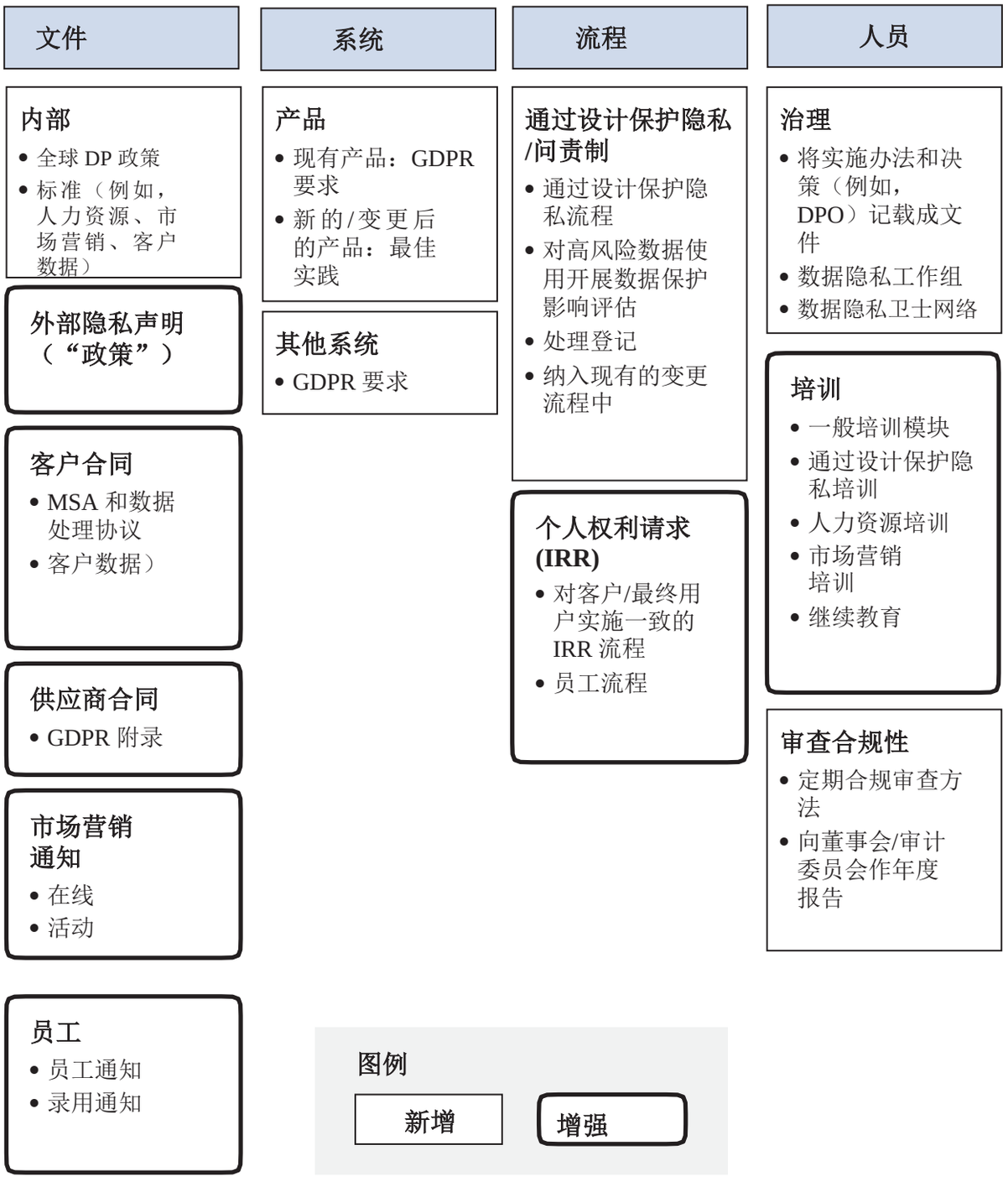
第 3 阶段 - 实施工作流

在最后一个阶段，我们将实施已确立的数据隐私文件并执行实施计划。我们将通过六个主要工作流完成实施：

1. 执行各职能单位和产品组的实施计划
2. 审查和更新面向公众的政策、通知和同意
3. 加强治理（角色和职责、培训、通过设计保护隐私等）
4. 审查和更新供应商合同（根据需要）[15]
5. IT 系统变更（根据需要）
6. 建立数据处理登记表

变更概述

下图概括了我们对完成实施活动后达到的 GDPR / 数据隐私计划的最终状态的设想。在实施 GDPR 后，我们将继续推进创新并适应变化以进一步完善我们的数据隐私实践。



我们的 GDPR 计划对您有哪些帮助？

Blackboard 的全球数据隐私 / GDPR 实施计划主要旨在支持贵组织实施 GDPR。下文将进一步详细阐述，但总体而言，主要包括以下 7 大要点：

1. **GDPR 就绪产品：**我们实施产品要求，以支持客户满足透明性要求、个人权利请求等。
2. **通过设计保护隐私：**我们实施通过设计保护隐私和数据保护影响评估 (DPIA) 流程，以促进制定合规性文件
3. **数据传输：**我们将继续实施多层方法：区域化、欧盟 - 美国隐私盾和经欧盟核准的示范条款
4. **和客户订立合同：**我们在标准主协议上补充了满足 GDPR 要求的数据处理附录
5. **我们的供应商：**我们制定了可靠的合同和供应商风险管理框架
6. **安全：**我们不断改进已确立的政策、程序和治理模式，以保护客户数据的安全
7. **泄露通知：**我们制定了以文件记载并经过检验的安全事件响应流程

1. GDPR 就绪产品

为客户提供 GDPR 就绪产品是我们的实施工作流的其中一个重要部分。为此，我们针对我们的产品设计了最低 GDPR / 数据隐私要求。和我们在全球范围内加强数据隐私实践一样，大部分要求适用于我们的所有产品，而不是仅限于在欧盟提供的产品。这也将为 GDPR 适用的位于欧盟以外的客户提供帮助。

通过可靠集中的流程，我们确立了自己的 GDPR / 数据隐私产品要求。我们和外部法律顾问一起拟定了一个初步版本。与我们的产品开发和产品管理团队的重要相关人员进行多次工作会议讨论和修改后，我们将该版本改进为具体且切实可行的一般产品要求并包含详细指导。GDPR/数据隐私产品要求后来转化为各产品组的产品实施计划中针对各产品实施的具体行动。

我们的产品要求[16]可以归为以下几类：

透明性

- 客户可以关联到他们的隐私政策/通知
- 提供关于个人信息一般会在产品中如何使用的信息

数据最小化 / 删除

- 审查产品的非必需/选填字段
- 审查产品是否可以使用虚构或匿名数据代替个人信息
- 可以按照客户的请求删除个人信息（当客户/用户无法自行删除数据时）

一般个人权利

- 在个人提出请求的情况下，可以提供对个人信息的访问权限和更正个人信息
- 在个人提出请求的情况下，可以删除个人信息

欧盟个人权利

- 可以处理数据迁移请求（个人在特定情况下收到机器可读格式的信息的权利）
- 可以停止使用个人信息（在特定情况下提出反对/限制的权利）

Blackboard 已经确立了符合 GDPR 要求的产品安全计划。因此，我们不额外制定特定于 GDPR 的安全要求。[17]

2. 通过设计保护隐私

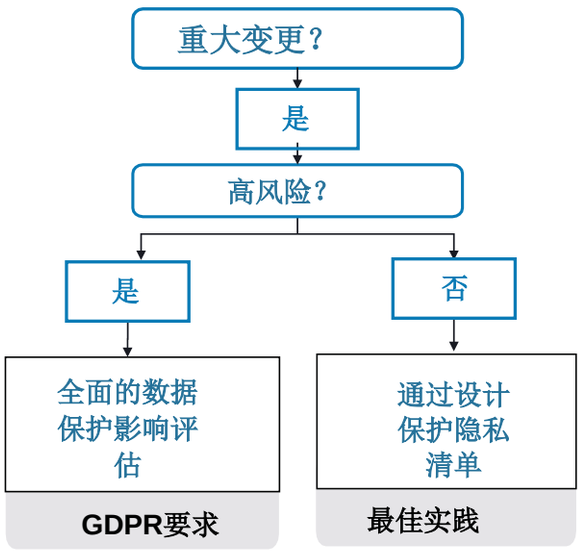
在当今世界，随着个人保持对其信息的控制权越来越难（见我们的隐私日博客文章中关于此主题的论述），通过设计保护隐私和问责制对于维护个人、客户和监管机构的信任以及用文件记载公司如何遵守 GDPR 越来越重要。因此，我们以通过设计保护隐私的方法为核心制定了全球数据隐私 / GDPR 计划。

对于 Blackboard 而言，这是一次改进，而不是改革。我们一直都对我们的新产品和实践开展法律审查。而通过设计保护隐私的方法，我们将这些审查日渐正式化，也更加文件化。

办法

- 我们创建了以文件记载的通过设计保护隐私流程和清单。
- 各职能单位和产品组将通过设计保护隐私清单纳入他们的变更流程中。
- 在个人信息的使用方式上每做出一处重大变更，都必须填写通过设计保护隐私清单。尽管 GDPR 未明确要求，但这是最好的做法。
- 对于高风险使用个人信息的情况，清单将触发更加详细的数据保护影响评估 (DPIA)（GDPR 要求）。

下面的流程图直观地描述了这一办法：



3. 数据传输

对于能够如何将个人信息传输到欧盟/欧洲经济区以外，GDPR 没有做出任何重大变更。现行的限制和数据传输机制仍然保留不变。这意味着如果实施了经欧盟核准的诸如欧盟 - 美国隐私盾或经欧盟核准的示范条款（数据传输协议）等数据传输机制，则可进行数据传输。这些机制确保个人信息在离开欧盟/欧洲经济区后仍然得到充分保护。

我们将继续采用分层冗余方法保证数据传输的合规性。这意味着我们通过多种途径满足数据传输要求，以确保对您的信息提供适当的安全保护：

- **区域托管：**我们实施区域托管战略，几乎全部产品在欧盟托管，其余少量产品将移至区域托管解决方案。尽管 GDPR 不要求进行区域存储，但我们认为数据本地化不会提高数据隐私或安全性，[18]而且我们了解许多欧盟客户更愿意其数据存储在欧盟。
- **隐私盾：**Blackboard 已通过欧盟 - 美国隐私盾认证，因此我们可以合法地将个人数据传输至美国。
- **示范条款：**我们还使用经欧盟核准的“示范条款”协议，这允许我们合法地将个人数据传输到欧洲经济区以外的其他国家/地区的 Blackboard 公司集团内部（“客户数据传输协议”）。
- **供应商：**我们与供应商和合作伙伴（例如，IBM、Amazon Web Services）订立了严格的合同，以确保将数据传输要求（以及其他数据保护义务）传达到我们的供应商和合作伙伴。

我们目前[19]有多个区域数据中心协助我们的欧盟客户在欧盟境内处理数据：

- 管理托管（Blackboard 数据中心）：阿姆斯特丹（荷兰）和法兰克福（德国）数据中心。
- 云托管（AWS 数据中心）：AWS 德国法兰克福区域（欧盟 - 中央 - 1）。

AWS 数据中心满足包括从 ISO 27001 和 ISO 27018 到 SOC2 在内的多项认证和要求，符合 GDPR 以及德国 C5 和 IT - Grundschutz 等地方要求。[20]

需了解的是，虽然大部分产品（包括Learn 9.1、Learn SaaS、Open LMS 和 Collaborate）的欧盟客户的客户个人信息存储在这些数据中心，但为了提供产品和服务（例如，提供 24 小时全天候支持），可能需要从欧盟/欧洲经济区以外的其他国家/地区访问这些数据。凭借上述欧盟 - 美国隐私盾认证和示范条款，我们可以进行此等数据传输。

4. 和客户订立合同

最新指令要求数据控制者和供应商（数据处理者）订立合同，但对于合同内容没有作详细要求。GDPR 的规定更加详尽，并且列出了必需内容。[21]

我们最新的标准数据处理附录包括下列所有必需要点。这些内容自动包括在我们和受 GDPR 所管辖的客户签订的标准主协议中。

- ✓ 仅可按照指示使用个人数据
- ✓ 职员必须签署保密协议
- ✓ 需实施适当的安全保护措施
- ✓ 聘请供应商（次级处理者）必须满足以下条件……
  - 获得数据控制者的授权（可以获得一般授权）
  - 以合同的方式要求遵守相同的数据保护义务
- ✓ 协助控制者回应个人权利请求
- ✓ 协助控制者实施安全措施、发出泄露通知和执行数据保护影响评估
- ✓ 在合同结束后归还或删除数据
- ✓ 提供数据控制者遵守规定所必需的信息
- ✓ 如果数据控制者的任何指示违背了 GDPR 要求应立即告知数据控制者

5. 管理我们的供应商

Blackboard 聘请供应商（例如，IBM、Amazon Web Services）协助我们向客户提供产品和服务。在此过程中，当需要访问客户的个人信息时，Blackboard 对供应商的数据隐私做法负责。

在我们的 GDPR 计划中，我们将通过设计保护隐私方法与现有的供应商风险管理和聘请流程紧密结合在一起，因而确立了以下重要控制措施：

- 和第三方订立包含隐私和 GDPR 附录的严格合同，其中包含的规定与我们和客户之间订立的合同基本相同
- 基于“示范条款”协议和 / 或 GDPR 和隐私盾附录合法地向供应商传输数据
- 制定供应商风险管理政策和框架文件
- 新供应商访问个人信息需填写供应商安全评估问卷，其中包括数据隐私合规问题
- 供应商访问由 Blackboard 管理的系统必须遵守 Blackboard 内部访问控制以及身份和授权政策，适当时还包括帐户审查
- 供应商需通过经核准的机制（例如 VPN）访问 Blackboard 资源
- 供应商对流量、用户和资产具有有限的访问控制

6. 安全

GDPR 在保护个人信息所采取的技术性和操作性措施（“TOM”）方面没有重大变化。此等措施需和在最新指令下所涉及的风险“相称”。因此，我们继续依赖于我们已确立的信息安全计划。

管理信息安全风险

我们确立了政策、程序、治理模式和技术要求以管理业务范围内的 IT 安全风险。

Blackboard 职员在入职的第一天就必须了解其在保护客户个人数据方面的责任：

- 了解保护敏感信息的政策
- 每年接受用户安全和数据隐私培训
- 网络钓鱼训练
- 知识公告板

我们规定了以下关于我们的员工在保护数据方面的要求：

- 界定了数据分类以及保护各数据类别的相应要求。客户的数据——学校机构及其学员的数据，具有最高级别的敏感性。
- 采取技术性控制措施保护数据的安全，例如：
  - 使用加密
  - 及时进行安全更新
  - 加强身份验证控制
  - 恶意电子邮件和网站通信保护
  - 端点保护技术
  - 基于知情需要限制访问权限

不止步于 GDPR……

作为一家为教育界服务的全球性公司，我们密切关注特定于相关地理区域和教育界的数据隐私和安全法律法规。

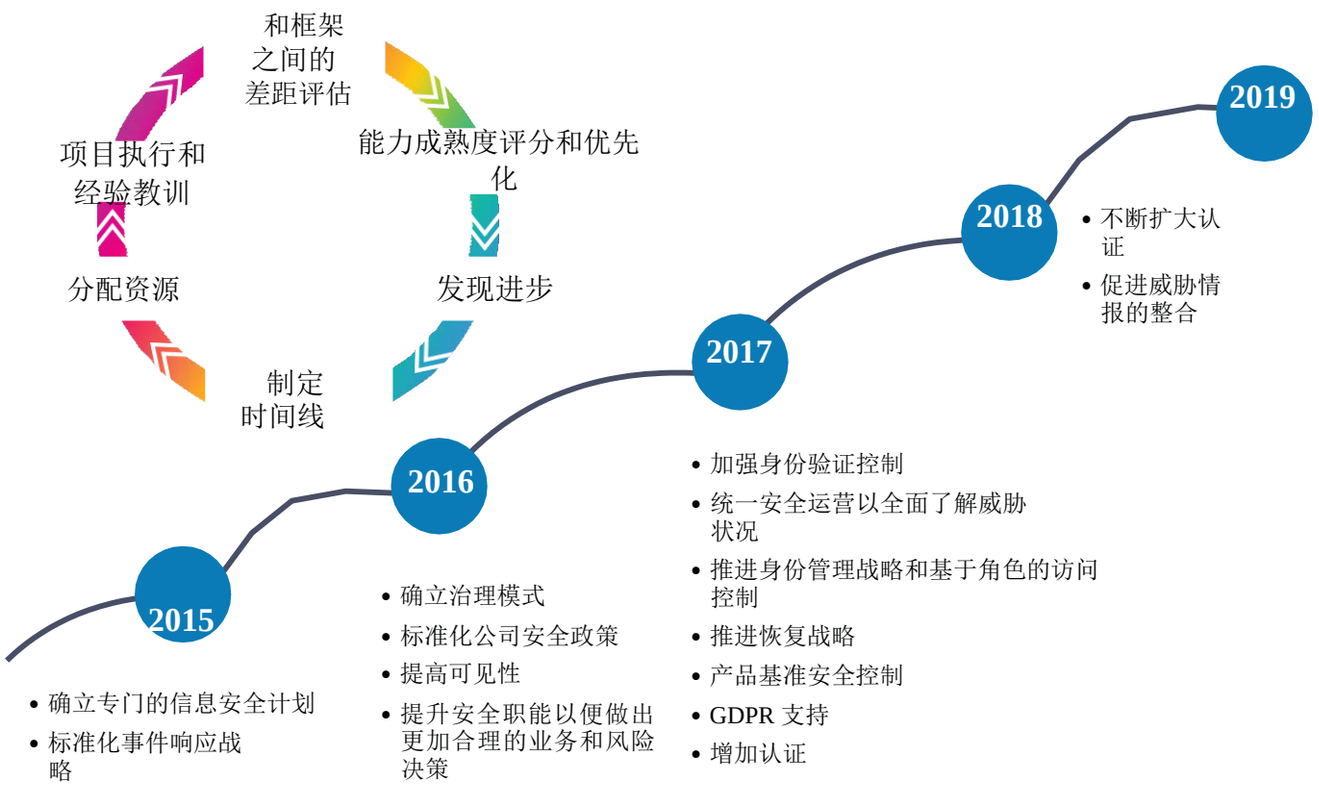
下面仅列出了 Blackboard 在制定安全政策、流程和技术控制措施时所考虑的除 GDPR 以外的其他安全和数据隐私法规、标准和框架的一部分例子。

- 美国《家庭教育权利和隐私法案》(Family Education Right and Privacy Act, FERPA)、《保护学生权利修订案》(Protection of Pupil Rights Amendment, PPRA)
- 美国《儿童网上隐私保护法案》(Children’s Online Privacy Protection Act, COPPA)
- 美国各州法律（现有的和新出现的 50 个州混合）
- 美国政府标准 - 联邦风险与授权管理计划 (FedRAMP)
- 支付卡行业 (PCI) 数据安全标准（根据适用情况）
- ISO / IEC、OWASP、NIST
- 国际标准 (MTCS, IRAP)

安全成熟度评估和路径图

我们努力不断完善我们的技术性和操作性安全措施。
下一页的图直观地描绘了我们持续进行的成熟度评估和路径图。

实施框架：安全成熟度评估和路径图



7. 泄露通知

GDPR 的其中一个重要变更是新增了一项规定，即强制要求将个人数据泄露情况通知相关数据保护机构，并且（在某些情况下）还应通知给相关个人。[22]

对于我们的大部分产品和服务，Blackboard 承担的是 GDPR 所定义的数据处理者[23]的角色。因此，将牵涉到 Blackboard 的泄露事件通知给数据保护机构和相关个人是我们客户的责任。但是，GDPR 要求 Blackboard 这样的数据处理者在此等情况下无不当延迟地（即“及时”）[24]通知给其客户（数据控制者）。

我们通过以下措施协助我们的客户在 Blackboard 发生和客户相关的个人数据泄露事件时履行其义务：

- Blackboard 安全事件响应 (SIR) 流程
  - 制定成文并定期检验
  - 协助在发生事件时迅速甄别、调查和补救
  - 允许及时通知客户
  - 依赖于已成立的安全事件响应团队（包括首席信息安全官和全球隐私官）
- 我们的最新标准主协议和数据保护附录[25]中明确规定了我们有及时通知客户的义务

结论

GDPR 要求重大变更从实行日期 2018 年 5 月 25 日起开始生效。我们希望本白皮书有助于您顺利实施 GDPR，也希望本白皮书体现了 Blackboard 对 GDPR 和数据隐私合规的重视程度。

下一节提供了其他有用信息，并列出了我们的联系电子邮件，以便您对本白皮书有任何疑问或反馈时可以联系我们。

GDPR 实用资源

下面的链接资源只是在线提供的有用资源的一小部分。它没有详尽列出所有可用资源。

若要了解 GDPR 对您的适用性的详细分析，还应咨询专家建议。咨询资深的数据保护专家（例如，您选择的律师事务所）非常重要。

欧盟官方资源

- GDPR 文本
- 第 29 条工作组指南
- 欧盟委员会 GDPR 网站

欧盟数据保护机构材料

- 英国信息委员会办公室 (ICO) 建立了一个完善的 GDPR 网站，提供以简洁语言编写的有用材料，且这些材料在持续更新
- 爱尔兰数据保护委员会 (DPC) 建立了专门的面向组织的 GDPR 网页
- 法国 CNIL 提供了一些英语材料，包括免费的隐私影响评估软件（以及大量法语材料）
- 西班牙 AEPD 编制了教育机构指南（PDF，西班牙语）

法律事务所指南

- Bird & Bird GDPR 指南
- Bird & Bird 会员律师事务所跟踪工具（跟踪全国 GDPR 变化）
- Linklaters GDPR 生存指南 (PDF)
- White & Case GDPR 手册

其他组织

- JISC 英国提供了关于 GDPR 的有用资源、活动和博客更新
- UCISA 发布了 GDPR 最佳实践文档，其中包括实践措施和案例研究
- 国际隐私专家协会 (IAPP) 提供关于欧洲数据隐私发展动态的非常有用（且免费）的每周资讯
- IAPP 还发布了实用的数据隐私工具提供者概述 (PDF)
- Amazon Web Services 成立了专门的 GDPR 中心

简历介绍

Stephan Geering

全球隐私官

- 负责全球范围内的数据隐私和安全法律合规
- 领导全球数据隐私 / GDPR 实施计划
- 向首席法务官报告；Blackboard 法律组成员
- 位于伦敦

Stephan 的背景：

- 瑞士州数据保护机构律师/数据保护副局长 (2002 - 2008)
- 伦敦大学学院法学硕士 (2008 - 2009)
- 巴克莱银行隐私组副主任 (2010 - 2012)
- 花旗集团数据隐私运营 EMEA 区域主管 (2012 - 2014)
- 花旗集团 EMEA 和亚太地区首席隐私官 (2014 - 2017)
- CIPP/E 认证

Rebecca McHale

首席信息安全官

- 领导产品和基础架构安全战略
- 监督 Blackboard 网络安全治理
- 向首席产品官报告
- 位于华盛顿特区

Rebecca 的背景：

- 2016 年进入 Blackboard；近期合并了安全组，加强了安全组织在公司内的职责
- 伦敦大学皇家霍洛威学院离散数学和计算应用理学硕士
- Novetta 和 CSRA 网络计划前高级总监，主管美国政府和商业客户 - 例如，国务院、运输安全管理局 (TSA) 和联邦存款保险公司 (FDIC)

更多信息

您可以在我们专门建立的数据隐私和安全社区网页上找到更多信息。

我们还发布数据隐私资讯。如果您想获取我们的资讯或对本白皮书有任何疑问或反馈，请联系我们：privacy@blackboard.com。

资料来源

1 请参阅末尾的“GDPR 实用资源”部分以获取更多有关 GDPR 的详细指导。

2 我们选择使用“个人信息”一词代替“个人数据”，但它的含义和涵盖范围和“个人数据”相同。

3 数据控制者是指确定数据处理方式和目的的组织（如何使用个人信息及其原因）。

4 请参阅“我们及贵组织在 GDPR 中的角色”部分。

5 请参阅下面的“揭秘 GDPR”部分以了解有关数据传输的更多详情。

6 请参阅 ICO 的“数据保护法案简介”以获取有关法案的有用概述。

7 另请参阅英国 ICO 关于 GDPR 误解的博客文章。

8 另请参阅 WP29（草稿）关于条例 2016/679 下的同意的指南 (WP259) 和 ICO 关于同意的指南。

9 WP29 关于条例 2016/679 下的个人数据泄露通知的指南（WP250 修订版 01）。

10 另请参阅“数据传输”部分。

11 例如，参阅英国 ICO 的“为 GDPR 做准备 - 立即采取的 12 个措施”(PDF)。

12 另请参阅“揭秘 GDPR”部分。

13 请参阅“GDPR 实用资源”部分。

14 有关全球隐私官和首席信息安全官的更多信息，请参阅“简历介绍”部分。

15 作为欧盟 - 美国隐私盾认证项目的一部分，我们已经将必需的 GDPR 合同规定纳入到我们和具有欧盟个人信息访问权限的供应商（次级处理者）订立的合同中。

16 请注意，并非所有的产品要求适用于所有产品。例如，一些产品没有允许客户链接到其隐私政策/通知的用户界面。

17 请参阅“安全”部分以获取更多详情。

18 一旦网络或系统连接到互联网，数据的物理位置对安全威胁的影响极小甚至没有。请参阅 Amazon Web Services (AWS) 白皮书“数据驻留 AWS 政策观点”（具体参阅第 2 页和第 3 页）以了解对数据本地化的可靠论据。

19 截至本文发布之日。

20 请参阅 AWS 合规计划以获取完整的认证和合规列表。

21 GDPR 第 28(2) - (4) 条。

22 GDPR 第 33 和 34 条。

23 有关对数据处理者的角色的解释，请参阅“我们及贵组织在 GDPR 中的角色”部分。

24 请参阅上文的“揭秘 GDPR”部分以获取有关个人数据泄露通知的时间和流程的更多详情

25 另请参阅“和客户订立合同”部分。