VansonBourne

欧盟一般数据保护条例（GDPR）

您准备好了吗？

ca technologies

目录

前言和简介

前言

《一般数据保护条例》（General Data Protection Regulation，简称 GDPR） 是欧盟（EU）推出的一项已 协商多年的新法规。该法规被广泛视为 20 多年以来欧盟 数字隐私格局的最大变革 — 在当今不断发展的数字经 济中，出台明确的法律和政策比以往任何时候都更重要。

2016 年 6 月，英国举行了全民公投，最终投票表决脱离欧盟。公投结果对英国的组织意味着什么？他们还需要遵守 GDPR 吗？

此次调查中位于美国的受访者表示，对于欧盟外部的任何组织，无论其所属国家/地区是否为欧盟成员，如果想要在欧洲单一市场内进行贸易，从 2018 年 5 月 25 日起都必须遵守 GDPR。

尽管已存在这一协定，但本文指出，为确保 GDPR 合规 性，大西洋两岸均有大量工作要做。GDPR 对个人数据的 定义进行了扩充，这意味着 IT 部门与测试部门都必须绷 紧神经，保护测试与开发环境中个人数据的安全。

组织需要援手，CA Technologies 可以提供一系列解决 方案，助力组织在项目中遵守 GDPR，从而帮助企业在 当今全球化数字世界环境中获得竞争优势。

Christoph Luykx

EMEA 政府关系总监

CA Technologies

简介

CA Technologies 委托进行了一项调查，您可以在本文 中查看调查结果，了解各组织目前对 GDPR 的合规性需 求的准备情况。鉴于 GDPR 将对非生产环境中可以使用 的数据类型产生广泛的影响，CA Technologies 尤其希 望了解企业计划应对 GDPR 的方式，以及需要什么样的 流程和技术来为其提供帮助。

研究范围

本文以 Vanson Bourne 进行的一项研究的调查结果为 依据。访谈开始于欧盟宣布通过 GDPR 当周（2016 年 4 月）。调查共计进行了 200 次 B2B 访谈；受访者包括 167 名 IT 决策者（ITDM）和 33 名风险与合规决策者（RCDM）。其中，98 名受访者为组织 C 级高管，其余 102 名为高级经理。

受访者所在组织均有至少 500 名员工，全球年收入超过 10 亿美元，涵盖多个领域，包括：

- 金融服务（包括保险）
- 制造
- 零售、分销与运输
- 技术与电信
- 其他商业领域
- 公共部门

访谈采取在线形式在英国（75 次）和美国（125 次） 进行，访谈人选经过了严格的多层次筛查以确保参与者都符合要求。

主要发现

GDPR 将对组织产生影响

- 仅 46% 的受访者对 GDPR 有充分的了解
- 在了解更多信息后，十分之九（90%）的受访者认为 GDPR 将对其业务产生某种影响
- 89% 的受访者举出了至少一个因 GDPR 而负担加重 的业务领域

为 GDPR 做好准备尚需不少时日

- 制定一项 GDPR 合规性计划平均需要三个月，实施这项计划又需要三个月
- 计划在实施过程中平均要经过三次修订

大多数组织还没有为 GDPR 做好准备

- 大约十分之三（31%）的受访者称其组织的测试实 践完全合规
- 不到半数（46%）的受访者称充分相信其组织可以及时做好准备
- 仅三分之一（33%）的受访者对快速识别所有系统及应用程序中的每一例客户数据非常有信心
- 大约十分之四（41%）的受访者认为组织设置了足够的粒度来限制数据的访问权限
- 仅 34% 的受访者完全有信心可以“毫不延误”地清理客户数据
- 仅 43% 的受访者完全有能力向客户提供其可访问 格式的数据，并且数据能够以其它格式传播

要满足合规性，组织需要加大技术投资

- 88% 的受访者称存在一些会引发合规性风险的 技术挑战
- 近十分之九（88%）的受访者认识到组织需要投资新的技术或服务，以便帮助其为应对 GDPR 的影响 做准备
- 58% 的受访者认为需要对加密技术进行投资
- 18% 的受访者当前还未使用合成数据生成，但可 能会在 GDPR 的影响下采用该技术

对 GDPR 的了解

欧盟（EU）最近通过了一项新法规 —《一般数据保护 条例》（GDPR），旨在加强对组织持有的个人数据的保护力度。该法规将于 2018 年 5 月生效，届时起全球所有 持有源自欧盟的个人数据的组织都需要完全遵守该法规，因此各组织现在就应该行动起来，对其用于管理数据的系统进行评估。

在正式采用 GDPR 当周（2016 年 4 月），仅 46% 的 受访者称对 GDPR 有充分的了解，47% 的受访者表示对 该法规了解不多，承认需要丰富相关知识。

GDPR 对业务的影响

显然，受访者的诸多业务领域都将受到 GDPR 的冲击。 了解 GDPR 的定义后，许多受访者表示该法规将对其组 织产生巨大的影响。至少十分之九的受访者称以下方面将会受到“一定”的影响（图 1）。

GDPR 的影响

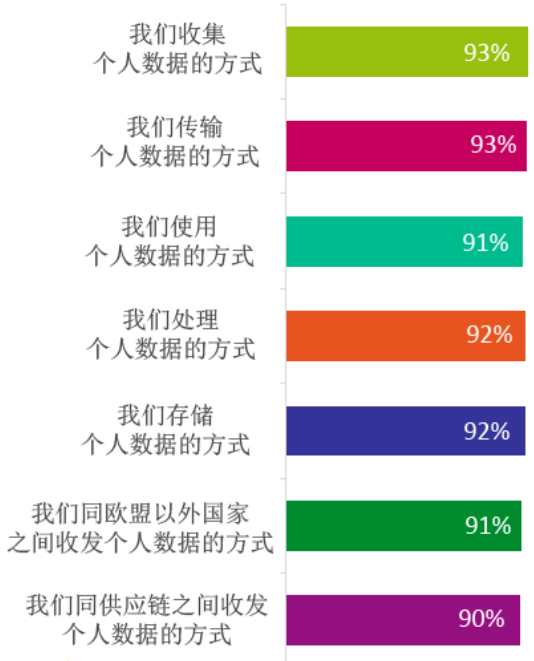

图 1：认为某领域会对业务产生影响的受访者所占比例分析。*200 名受访者均被问到了这一问题*

受访者对 GDPR 了解得越充分，他们预计 GDPR 对业务 的影响就越大。对 GDPR 了解不多的 IT 决策者（ITDM）及风险与合规决策者（RCDM）还没有意识到该法规会对 其组织产生多大影响。这种认知对确保组织能够在 GDPR 生效（2018 年 5 月 25 日）前及时做好准备是至关重 要的。

不断变化的法规对许多组织都是一种负担

近十分之九（89%）的受访者举出了其组织中至少一个因 GDPR 而负担加重的领域。事实上，对 GDPR 有充分了 解的受访者中，高达 96% 的人称组织负担加重，与此相 比，对 GDPR“不是很了解”或“完全不了解”的受访者中仅 33% 的人这样说。由于对 GDPR 缺乏了解，这些组织如 果知晓他们为确保合规性而需要做多少工作，很可能感到震惊。

受访者谈得最多的一个负担就是，组织要为 GDPR 消耗 大量的 IT 资源和员工时间（60%）。IT 部门比风险与合 规部门更倾向于认同这一点（分别占各自人数的 66% 与 30%）。

此外，受访者还认为培训资源（38%）与培训预算（37%）也很可能受到影响，然而 34% 的受访者表示其 组织未来没有充足的培训资源和预算来实现 GDPR 合规性。

美国与英国

尽管这是一项欧盟法规，英国与美国的受访者中对 GDPR 有充分了解者却占到相似的比例 （分别为 45% 与 46%）。

英国的受访者更倾向于认为 GDPR 会造成资源负担。93% 的英国受访者称满足不断变化的 一般数据保护法规要求 — 及其相关规定 — 在某种程度上就是一种负担，与此相比，87% 的美国受访者认同这一观点。

为 GDPR 做准备

为 GDPR 实施合规性计划

部分受访者所在的组织已经落实了全套合规性计划，他们表示制定该计划平均需要三个月，实施该计划平均又用了三个月。尽管这加起来才六个月，大部分（54%）受访 者对于测试这一单项能否在两年的实施期内满足合规要求却并非很有信心。

至于那些已经着手制定计划（但未必已完成 GDPR 合规 性计划）的组织，据其受访者描述，到目前为止他们平均已经对计划进行了三次部分修订。这一点可能促成 89% 的受访者称满足不断变化的一般数据保护法规要求及其相关规定对组织就是一种负担。

尚未开始制定合规性计划的组织需要尽快着手，以确保在最后期限前能够满足合规性要求。

GDPR 合规性带来的技术挑战

满足 GDPR 合规性并非易事。近十分之九（88%）的受访者称存在一些会引发合规性风险的技术挑战超过半数（54%）的受访者称组织内部存储敏感数据的方式没有 统一。

相比风险与合规部门的受访者（70%），IT 部门的受访者（92%）更倾向于认为未来将面临会引发合规性风险的技 术挑战。事实证明，IT 部门对技术挑战有更深刻的认识，但风险与合规部门应加深对合规性风险的了解。不管 怎样，两个部门的大多数受访者都认为存在挑战。

引发合规性风险的技术挑战

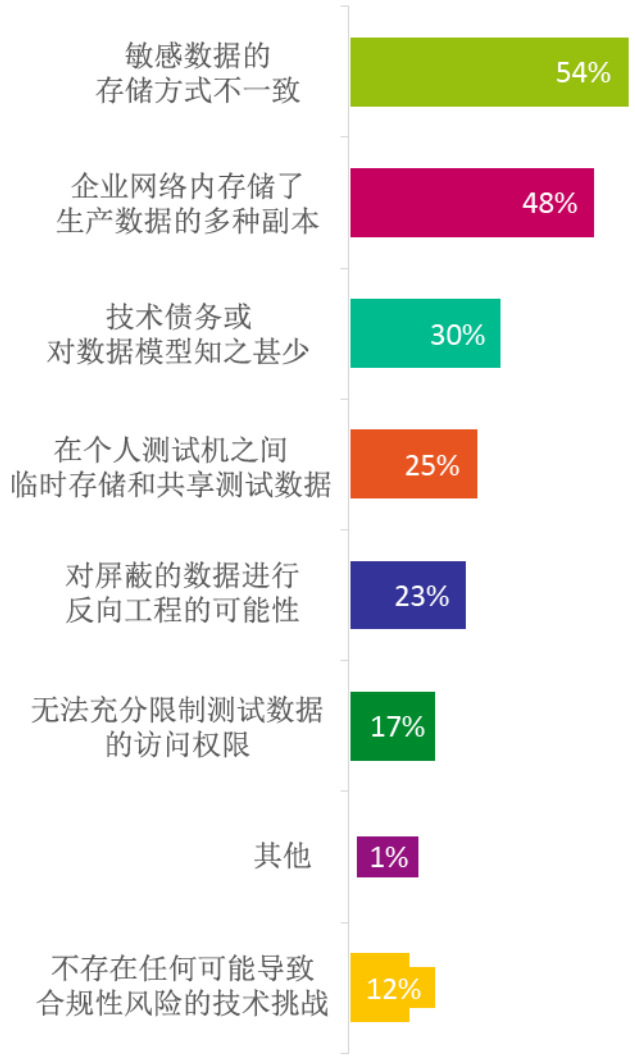

图 2：“哪些技术挑战可能会给贵组织带来合规性风险？”*200 名受访者均被问到了这一问题*

绝大多数（88%）的受访者称组织面临着一些会引发合规性风险的技术挑战。最大的挑战就是如何正确地存储敏感数据（54%）

当前的 GDPR 合规性障碍

当前的测试实践尚不达标

仅十分之三（31%）的受访者称其组织当前的测试实践在技术、程序和文化方面都遵守 GDPR。大多数组织要完成大量工作才能满足合规性要求。他们只剩不到两年的时间来确保落实到位。

当前合规程度

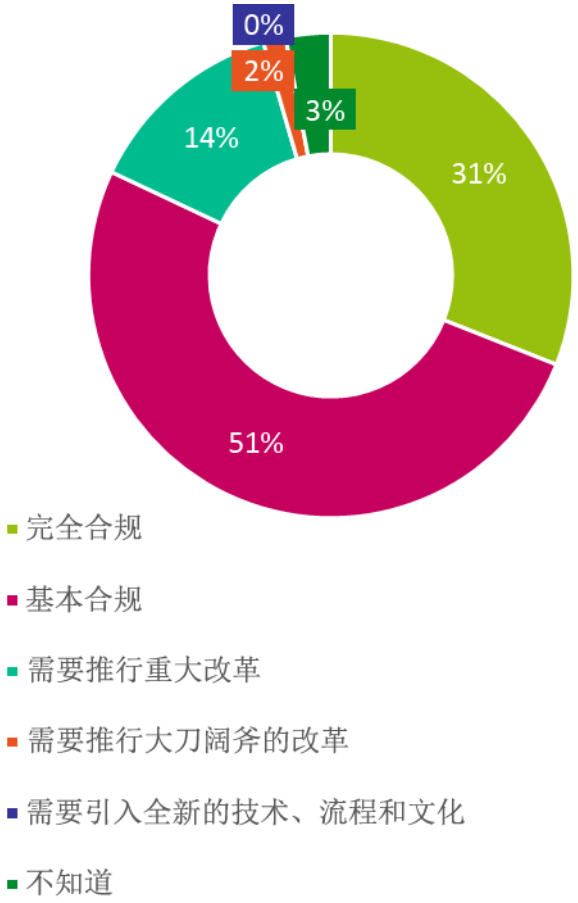

图 3：“您认为贵组织当前的测试实践在技术、程序和文化方面对 《一般数据保护条例》的遵守达到怎样的程度？”*200 名受访者均被问 到了这一问题*

然而，只有不到半数（46%）的受访者称充分有信心在实施期内达到合规性标准。这说明大多数组织都担心不能在 2018 年 5 月 25 日这一最后期限前做好准备。

C 级高管（52%）受访者更倾向于对其组织在最后期限前做好准备充满信心，与此相比，只有十分之四（40%）的高级经理对其组织有这样的信心。

在整个调查中，C 级高管和高级经理的观点存在差异， 这可能是因为高级经理更多的时候需要在前线冲锋陷阵，对现实大概也比 C 级高管看得更加清楚，而 C 级高管更 倾向于认为他们所希望的就是真实情况。

当前流程中合规性差距

大多数受访组织的流程目前都不符合 GDPR。

仅三分之一（33%）的受访者对快速识别组织中存在的系统及应用程序中的每一例客户数据非常有信心。这意味着大多数受访者对其组织现在能否完成这一任务不是很有信心。42% 的 C 级高管受访者对在组织中完成这一任务非常有信心，与此相比，仅 25% 的高级经理对其组织有这样的信心。这些 C 级高管是单纯抱有如此美好的愿望，还是说他们不知道这项任务的要求有多高？

仅 41% 的受访者称当前的流程和技术能够将数据访问限制到该法规要求的程度。同样，这意味着大多数组织在这方面还没有为 GDPR 做好准备。C 级高管似乎更倾向于 认为其组织在此方面已满足合规性要求，其中超过半数（50%）持有这样的观点，与此相比，仅约十分之三（31%）的高级经理认同这一说法。这进一步表明，C 级 高管在其组织是否为 GDPR 做好了准备这一问题上可能 过于乐观了。

“毫不延误”地清理客户数据

GDPR 的重要特征之一是“被遗忘权”，即赋予数据主体（如客户）要求数据管理方（如组织）在某些情况下清除其个人数据的权利。

仅约三分之一（34%）的受访者完全相信其组织能够在客户提出要求时毫不延误地清理掉客户的每一例（测试）数据。此外，43% 的受访者对组织有一点信心，但不确信 是否能够清理彻底，而这就违反了该法规。这再次说明，大多数组织还有工作要做才能确保符合 GDPR。

清理数据

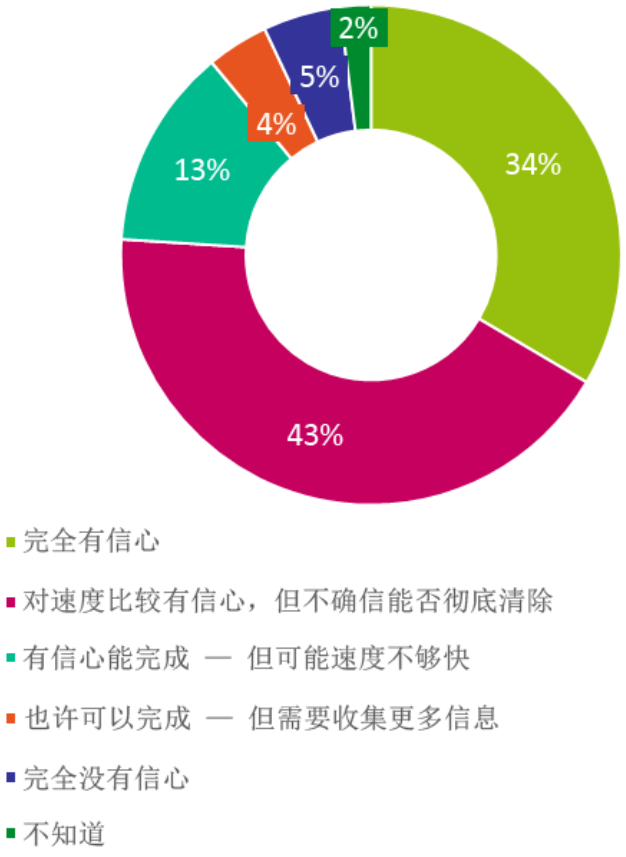

图 4：“如果客户要求‘毫不延误’地清理掉他们的每一例个人（测试）数据，您目前对贵组织完成这一任务抱有多大信心？”*200 名受访 者均被问到了这一问题*

允许客户访问其数据

GDPR 的另一主要特征是“数据可移植权”；数据主体将能够在服务提供商之间传输个人数据，而组织必须实现这一点。

如果客户要求访问他们的每一例数据，数据要呈现为他们可访问的格式并且能够以其它格式传播，仅 43% 的受访者表示其组织现在可以完全满足这一要求。相似比例（44%）的受访者表示可以实现这一点，但是仅限一到两 种格式，可能不是客户想要的格式，甚至无法读取。 此外，十分之一（10%）的受访者现在根本无法满足 这一要求。这又再次证明，组织需要改变工作方式才能 符合 GDPR。

美国与英国

对于组织是否将及时做好准备，以及目前是否已经满足合规性要求，美国受访者都比英国受访者更有信心。美国受访者更倾向于：

- 充分相信测试能够在两年实施期内达到合规性要求 — 49% 的美国受访者有这样的信心，与 41% 的英国受访者形成对比
- 对快速（十个工作日内）识别组织中存在的系统及应用程序中的每一例客户数据非常有信心 — 38% 的美国受访者有这样的信心，与 24% 的英国受访者形成对比
- 通过足够的粒度来限制数据访问 — 44% 的美国受访者这样认为，与 35% 的英国受访者形成对比
- 完全相信当前能够“毫不延误”地清理掉每一例个人（测试）数据 — 36% 的美国受访者有这样的信心， 与 29% 的英国受访者形成对比
- 能够以客户可访问的格式提供数据并且能够以其他格式传播 — 47% 的美国受访者这样认为，与 36% 的英国受访者形成对比

技术助力 GDPR 合规性

对技术投资的需求

近十分之九（88%）的受访者认识到组织需要投资更多技术才能遵守 GDPR。他们打算在各个方面增加投资，包括加密技术（58%）、分析和报告技术（49%）以及测试数 据管理（47%）。

近十分之四（39%）的 C 级高管受访者预计需要巨额投 资，与此相比，高级经理中持此观点者不到这个数字的一半（16%）。鉴于 C 级高管更倾向于认为其组织在多个 方面都已经满足合规性要求，这一结果出人意料。

技术助力测试环境中的合规性

许多组织已经落实（图 5 中的绿色部分）或正在计划落实（粉色部分）一些措施来帮助确保测试环境中的合规性。尽管尚未落实任何计划的组织占到一定比例，但值得欣慰的是，其中大部分明白应该落实（浅绿色部分为“应该落实”，橙色部分为“不需要”）。

尽管许多组织已经落实一些措施，但值得我们回顾的是，近十分之九（88%）的受访者称存在会引发合规性风险的技术挑战（图 3），并且超过半数的受访者称组织内部存储敏感数据的方式没有统一。

确保测试环境中的合规性

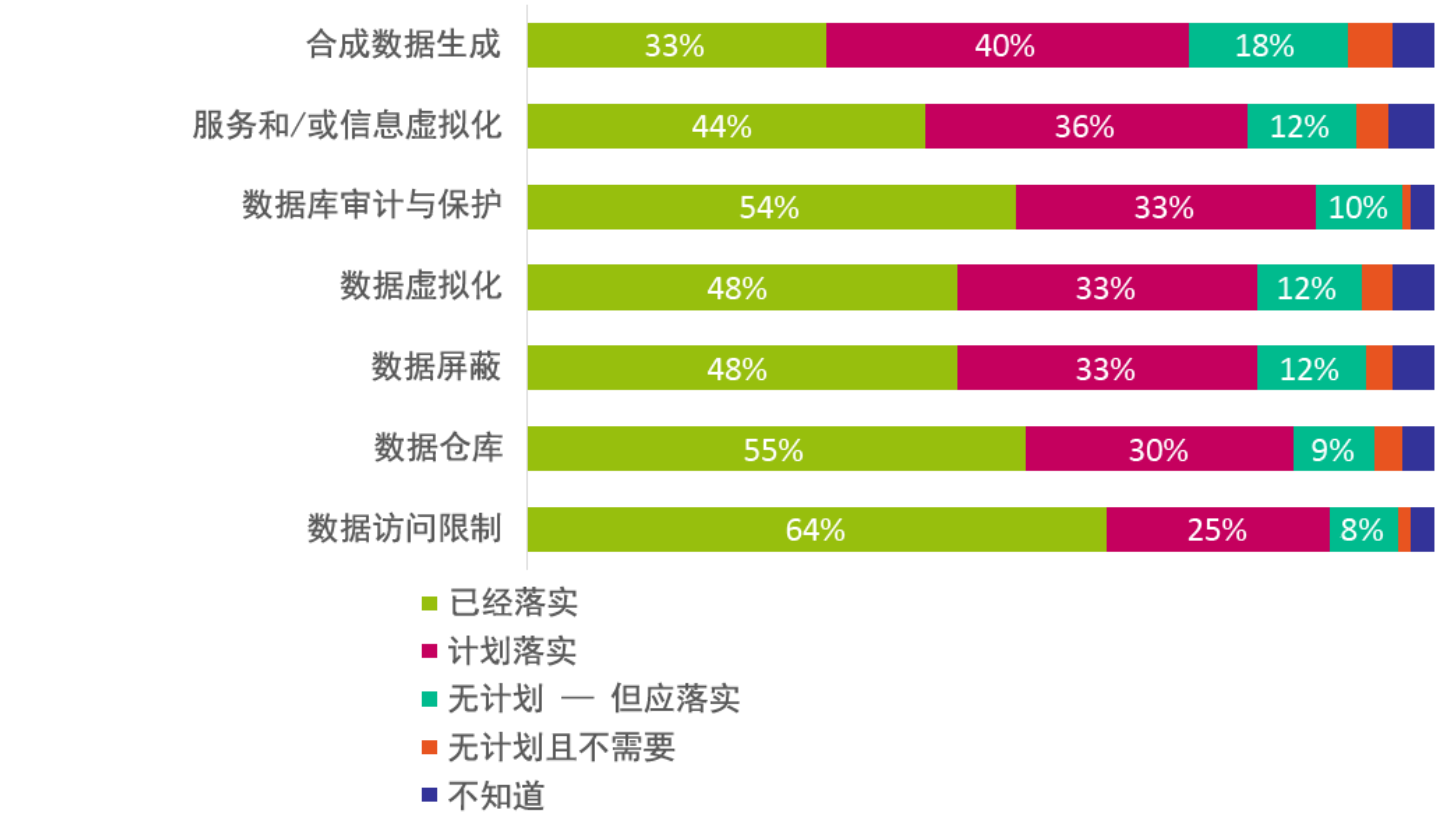

图 5：“为帮助确保测试环境中的合规性，贵组织当前已经落实哪些措施？或者您认为需要落实哪些措施？”*200 名受访者均被问到了这一问题*

使用合成生成的数据

仅 19% 的受访者所在的组织使用合成生成的数据（同时未使用屏蔽的数据），但另有 18% 受访者称可能会在 GDPR 的影响下采用该技术。

数据屏蔽与合成数据的组合将成为最常见的 GDPR 合规性解决方案。

近十分之六（58%）的受访者表示其组织将配合实施数据屏蔽与合成数据生成，以便满足 GDPR 中与个人可识别 信息的使用有关的合规性。

C 级高管（65%）受访者更倾向于认为其组织将配合实施数据屏蔽与合成数据生成来满足合规性。与此相比，仅刚过半数（51%）的高级经理称其组织有这方面的计划。

然而，7% 的受访者称其组织尚未决定或商讨将采取哪些行动来满足合规性要求。这些组织需要开始进行计划以确保在最后期限前满足合规性要求。

假名化

定义：对个人数据进行处理，使得在没有附加信息的情况下无法认定该数据出自某特定数据主体，只要将附加信息与数据分开存放，并且采用技术措施及组织措施，就可确保数据无法被认定为出自某个已识别或可识别的用户

在当前屏蔽数据的组织中，13% 的受访者尚未意识到可 能需要评估其组织的流程是否符合 GDPR 的要求。 此外，仅 39% 的受访者认为当前与假名化相关的流程和 技术可以达标。这再次说明，大多数组织还有工作要做才能符合 GDPR。

同样，C 级高管（46%）受访者更倾向于认为其组织在此方面已经满足合规性要求，与此相比，仅 31% 的高级经理认同这一说法。

对 GDPR 有较多了解的受访者更倾向于表示其组织当前 可以达标。深刻认识到 GDPR 影响的受访者可能已经在 组织内采取行动，为 GDPR 合规性做准备。

美国与英国

美国受访者更倾向于认同组织需要巨额投资 （31% 的美国受访者表示认同，与 20% 的英 国 受访者形成对比）。

然而，15% 的英国受访者表示将从数据屏蔽转向合成数据生成以避免使用任何生产数据，与 7% 的美国受访者形成对比。

结论

鉴于欧盟最近才正式宣布通过 GDPR，受访者们表现出合理的认识。在获悉该法规后，88% 的受访者称其组织将 在满足 GDPR 合规性要求的过程中面临技术挑战。受访 者都意识到需要完成大量工作才能满足合规性要求。

许多受访者透露了当前组织内部在 GDPR 合规性方面的 差距。既然大家都意识到将存在技术挑战，那么 88% 的受访者认为需要投资技术才能符合 GDPR 也就不足为 奇了。58% 的受访者将投资加密技术，此外相当一部分 认为可能在 GDPR 的影响下采用其它技术，例如在测 试数据管理解决方案中利用合成数据生成（18%）。

不断变化的的 GDPR 要求对受访者所在的组织是一种负 担；一部分组织已着手应对一些要求，但仍有大量工作要做。制定并实施（加上修订）一项 GDPR 合规性计划需 要六个月时间。如果组织不尽快着手制定合规性计划， 他们很可能无法在 2018 年 5 月这一最后期限前做好 准备。

组织应加强对新法规本身的知识普及 — 同时还需借助新技术。在各个方面都只有少数受访者对其组织的流程有信心或称其组织已经符合 GDPR 的要素。仅 31% 的受访 者认为其组织在当前测试实践方面完全合规。此外，仅 39% 的受访者认为与假名化有关的当前策略可以达标。 大多数组织还有工作要做才能确保合规性。

即使 GDPR 是一项欧洲法规，美国的组织也在准备应对 影响。这项法规将对全球范围的组织造成影响，难怪 31% 的美国受访者认为其组织将需要巨大的技术投 资来帮助满足 GDPR 合规性。

趁现在还来得及，所有组织都应尽快落实计划以符合 GDPR。

要了解与 GDPR 或贵组织可以采取的行动有关的更多 信息，请观看 CA 和 Vanson Bourne 的网络广播：

“Are You GDPR Ready?Get the Vanson Bourne Readiness Survey Results”

关于 CA：

CA Technologies（NASDAQ:CA）致力于开发促进企业转型的软件，为其抢占应用程序经济的先机。软件是各行各业的 核心。从规划到开发再到管理和安全性，CA 正与全球各地的公司开展跨移动、私有和公共云、分布式和大型机环境的 合作，以改变我们的生活、交易和沟通方式。要了解详情，请访问 ca.com/cn。

CS200-215379

关于 Vanson Bourne：

Vanson Bourne 是从事技术领域市场研究的独立专业机构。本着严谨调研的原则，凭借征询所有业务领域及主要市场中 的技术及业务职能部门高级决策者意见的实力，我们因健全可靠的基于研究的分析而建立起良好的声誉。有关更多信息，请访问 www.vansonbourne.com