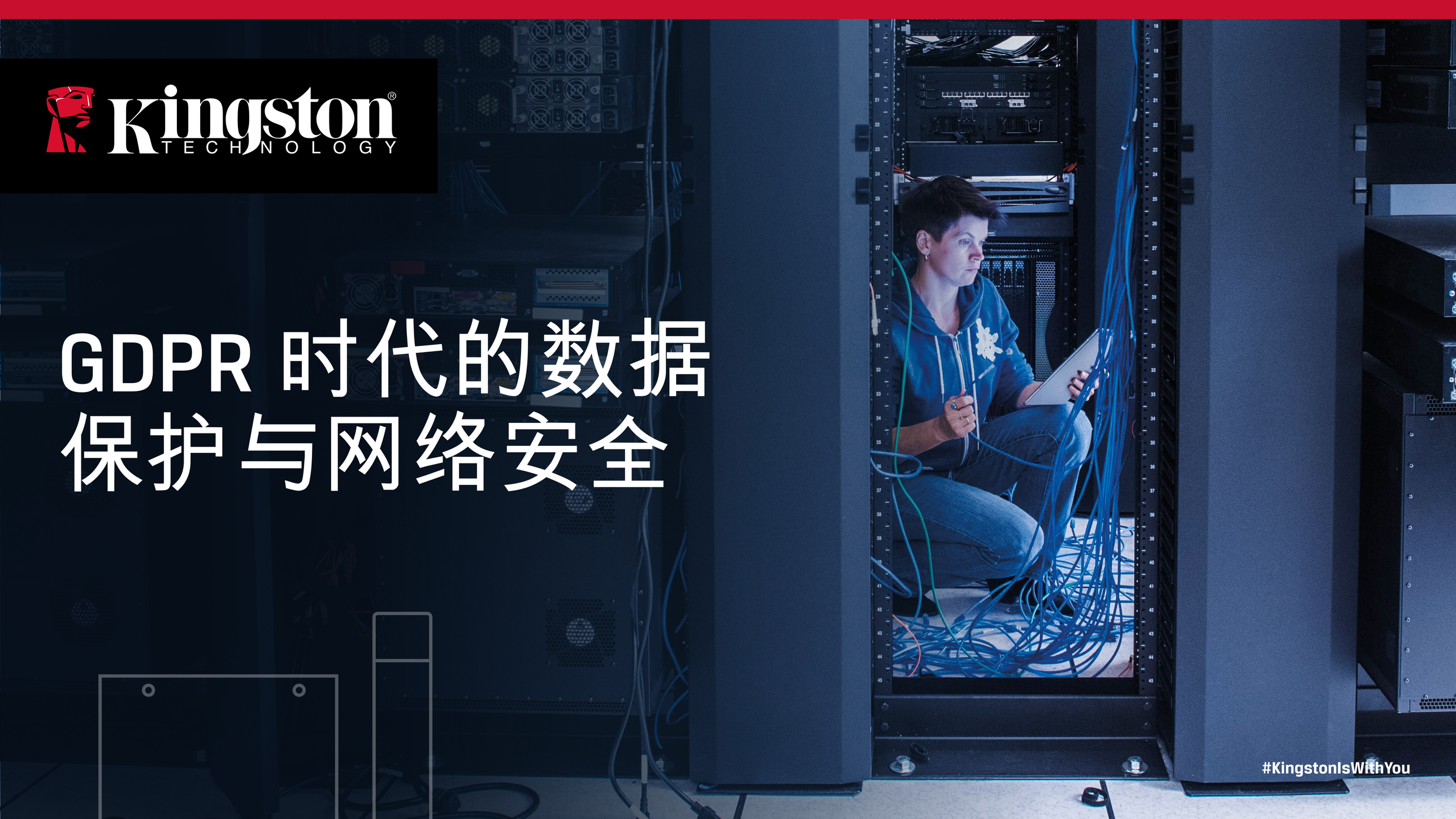


GDPR 时代的数据保护与网络安全

#KingstonIsWithYou

GDPR 时代的数据保护与网络安全

前言

为了准备好应对 GDPR，无数公司和组织纷纷努力采取举措并大肆招聘人才。或许，您也是其中一员。然而，面对不断演变的网络威胁，您根本没有机会停下来喘口气。GDPR 合规并非打勾练习，而是一个评估持续的数据保护和网络安全工作的框架。毫无松懈空间可言。

在这本短小精炼的电子书中，我们汇聚了英国网络安全领域最有经验的一些评论员的知识见解，探讨了 GDPR 实施以来数据保护发生了怎样的变化。我们还介绍了公司如何在合规需求方面对自己的员工进行培训，并讨论了 IT 部门和技术提供商可以如何更好地保护 IT 技术设施，以及在新兴安全挑战方面为最终用户提供指导。

GDPR 时代的数据保护与网络安全

撰稿人

这本短小精练的电子书由数据保护和网络安全领域的五名专家共同撰写。

Rob Allen
@Rob_A_kingston

Rob 担任金士顿科技公司营销与技术服务部门主管，自 1996 年起就一直效力金士顿。Rob 负责管理所有金士顿品牌和产品的公共关系、社交媒体、依托数字营销媒体与创意的渠道营销工作。

Tara Taubman-Bassirian
@clarinette02

Tara 集诸多头衔于一身：律师、倡导者、调停者、研究员、顾问、演讲家和作家。凭借在隐私、知识产权和数据保护等领域的卓越专业知识，她在世界许多地区享有盛誉，特别是在英国、法国和美国。

Rafael Bloom
@rafibloom73

Rafael 是 Salvatore ltd 主管。他负责帮助不同公司应对技术和法规调整带来的战略、商务和过程方面的挑战与机遇。

Miriam Brown
@Kingston_MBrown

担任金士顿科技公司 B2B 策略营销经理，自 1997 年起就一直效力金士顿。Miriam 负责所有金士顿 B2B 产品的营销策略、内容和宣传活动。

Sally Eaves
@sallyeaves

Sally Eaves 教授被誉为“道德科技的火炬手”。作为 Emergent Technologies 教授和全球战略顾问，她从首席执行官和首席技术官职位积累了深厚的经验。Sally 是一位屡获殊荣的国际主旨演讲家、作家、研究员和影响者，致力于分享原创、真实的思想领导力。

GDPR 时代的数据保护与网络安全

目录

第 1 章 – GDPR 实施以来数据保护发生了怎样的变化?

公司已经实现了长足发展。过去两年来，法务团队扩大，数据保护官招聘数量激增[1]，对外部数据隐私法律顾问的咨询量也增加。数以千计的企业现在熟悉数据保护影响评估 (DPIA) 的完成流程。

但是，路漫漫其修远兮。

GDPR 带来的一个最大挑战在于，您必须时时刻刻小心谨慎。在多数组织中，几乎任何员工随时都可能违法相关法规。在劳动力紧张或高度自治的领域，例如医疗保健、教育和法律，这个问题更为严重。举例来说，在法律领域，许多事务律师会毫不顾忌地通过简单的电子邮件附件交换敏感的案件细节。医疗保健专业人员利用不安全的电子邮件地址交换患者数据或核磁共振成像 (MRI) 扫描结果。在高压力的组织中，哪怕在任务清单中增加一点点压力，合规就不复存在。生产效率看起来会击败协议。

这种局面必须改变。

而且，慈善机构中存在意识问题。慈善机构似乎常常认为他们豁免 GDPR 的管制。即便他们确实理解 GDPR 适用于任何私人部门、公共部门和第三部门的组织，他们也不愿意把用于慈善事业的资金投入数据保护，尽管这可能合乎情理。

这种行为既高尚又天真。GDPR 违规招致的潜在罚款让很可能出现的 IT 开支相形见绌。

Tara Taubman-Bassirian
@clarinette02

GDPR、数据保护与知识产权顾问

“许多第三部门组织表示：‘GDPR 不适用于我们，我们只是慈善机构。'甚至在网站合规方面，我尝试告诉他们，关键不是您想收集的数据，而是您批准访问您的访客数据的第三方。”

2016 年以来

市场对于数据保护官 (DPO) 的需求激增，增幅超过 700%。

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [于 2019 年 11 月 26 日访问]

GDPR 实施以来数据保护发生了怎样的变化?

数据最小化是个鼓舞人心的趋势

我们生活在一个肆无忌惮收集数据的时代。“四大巨头”（Google、Apple、Facebook 和 Amazon）保留着海量的客户数据。不妨可以假设，其他组织也在模仿四大巨头，收集尽可能多的数据。而您保留的数据越多，您的风险敞口越大。GDPR 实施以来出现了一个最积极的趋势，即公司反对过多收集数据。明智的公司采用数据最小化原则：不需要则不收集。

Tara Taubman-Bassirian
@clarinette02

GDPR、数据保护
与知识产权顾问

“数据最小化很可能是 GDPR 最佳原则之一。任何数据库的创建都意味着创造风险。”

Rob Allen
@Rob_A_kingston

金士顿科技公司
营销与技术服务部门主管

“我们有严格的数据删除规则。当然，对于业务至关重要的数据必须正确存储。但其他数据呢？一年后就不复存在了。保留这类数据有何意义？”

由此带来的好处不只是限制风险。以市场营销为例。如果您的市场营销数据库不干净，就可能保留着过时数据。如果您的数据库达到数以万计用户的级别，当您执行频繁的电子邮件市场营销活动时，成本就会增加。它还会扭曲您的市场营销绩效统计数据。

数据最小化也适用于物理拷贝形式的数据。小心对待您打印的内容（例如客户护照扫描件）；小心对待您写下的内容（例如帐户密码）。当您确实需要保留数据的物理拷贝时，务必安全存放。桌上堆积如山的文件资料可能看起来令人印象深刻。但保护起来则是另一回事。

Rafael Bloom
@rafibloom73

Salvatore Ltd
主管

“对于技术与企业实际运营业务之间的结合点，我们见到了完全不同的思考方式。企业领导层亟需立即实现这种水平的数字化成熟度。”

风险敞口的影响：从高层管理人员到消费者

数据保护作为一个法规概念已经存在几十年了。但是，迄今 Google[1]、British Airways 和 Marriott 连锁酒店[2]等公司遭受的大笔罚款以及相关的媒体报道，让 GDPR 引起了高层管理人员的注意。这引发了涓滴效应。

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [于 2019 年 11 月 26 日访问]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [于 2019 年 11 月 26 日访问]

GDPR 实施以来数据保护发生了怎样的变化?

续...

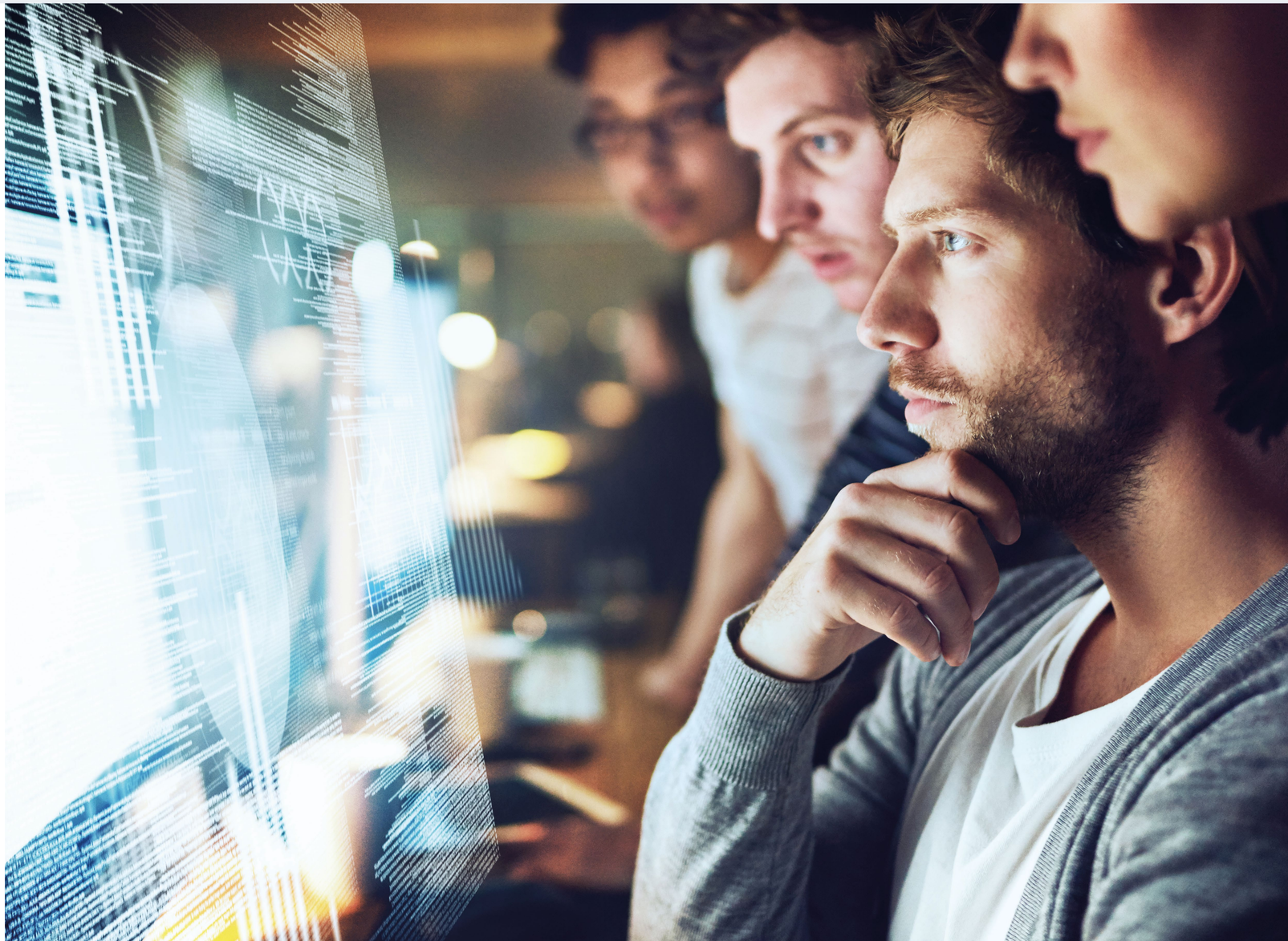
促使组织采取强有力数据保护的另一个驱动因素是协作业务。大型企业现在对潜在提供商数据安全的完整性执行广泛的尽职调查，因为他们不想为任何合作造成的数据泄露负责。

增强的 GDPR 商业意识还有另一面：消费者对他们数据权利的意识增强。他们知道，如果公司对他们的数据失去控制 – 注意：不一定是数据泄露 – 他们有权获得赔偿。企业必须保持专注。

Sally Eaves
@sallyeaves

Sally Eaves Consultancy
CEO、主管

“数据保护已成为企业的当务之急，决定企业赢得还是失去信任。”



第 2 章 – 组织如何对自己的员工进行培训?

员工培训：能让您的员工翻白眼的四个字。

确保培训吸引人又多了一个理由。经过培训的员工更不可能违反数据保护良好做法。即便出现数据泄露，如果您可以证明自己努力在数据安全方面对员工进行了培训，信息专员办公室 (ICO) 在裁定中对您的态度更加有利。

Rafael Bloom
@rafibloom73

Salvatore
主管

“我想把数据看作一个供应链项目，其中数据来源和数据整个生命周期需要得到妥当管理。把自己的团队叫到屋里培训半小时，告诉他们要做什么，例如请勿粉碎东西，请设置合适的密码，这不失为一个好方法。毕竟，您降低了组织面临的风险。但是，过些时间，除了一开始您从某种程度上强加给员工的影响力，真正实现重大改变了吗？并没有。”

不过，2019 年 4 月，英国数字产业部长 Margot James 表示，十分之三的英国组织对员工进行了培训，以应对网络威胁[1]。是时候认真对待培训了。

关键是形成文化，而非打勾培训

培训的关键是影响真正的行为和文化变化，而非打勾。组织很容易购买在线培训课程，包括一些任何人都可以回答正确的数据保护相关的简单问题。但这真的有助于保护您的组织吗?

良好的数据保护行为包含两个基本要素。第一，培训不仅智能、吸引人，还适合您组织面临的独特挑战。其次，认识到 GDPR 是个深刻的职场文化问题，每天都在影响全体员工。关键是在整个组织内以正确的方式利用数据做正确的事情。以人力资源为例。想想只是存储在电子邮件服务器中的所有员工候选人详细信息。数据保护人人有责。

1. Intelligent CISO: One year on, what has been the impact of GDPR on data security? www.intelligentciso.com/2019/04/16/one-year-on-what-has-been-the-impact-of-gdpr-on-data-security/ [于 2019 年 11 月 26 日访问]

组织如何对自己的员工进行培训?

数据背后就是人

在第一章，我们提到消费者对于他们数据权利的意识不断增强。要对数据保护培训进行定位，最好是帮助您的员工联想到，数据背后总有人存在。让您的员工思考从他们获取了数据的每个组织，他们会认识到数据保护的关键是个人隐私。

部署应急计划

Sally Eaves
@sallyeaves

“持续对员工进行数据安全与隐私方面的培训是企业的当务之急。这不应是一年一次的非经常性培训活动，而应是积极、互动、吸引人的体验，以便成为日常工作体验的一部分。员工必须参与关于我们希望规避、管理和捍卫什么的对话。”

Miriam Brown
@Kingston_MBrown

“我认为，在培训期间向员工讲讲以下内容将非常有趣：‘如果这是您的数据，会怎样？'如果我的银行经理利用他的笔记本电脑在家办公，并在这台电脑中存储敏感信息，我将希望信息存储在加密硬盘中。”

Rob Allen
@Rob_A_kingston

“就像对待自己的东西一样对待数据。”

第 3 章 –
IT 部门能否更好地保护设备？

远程办公是新常态

您的员工很可能从多台不同的设备访问工作环境，包括可能容易遗忘在火车或出租车上的个人设备。您的挑战在于找到一个妥善方法，既能帮助您的员工高效工作，又能让您避免安全风险和数据泄露。毕竟，只要一名员工就能让您的数据保护努力毁于一旦。

Sally Eaves
@sallyeaves

Sally Eaves Consultancy
CEO、主管

“数据需要在传输、静态和使用中得到保护，部署全方位的安全、恢复和数据擦除计划来涵盖所有这些场景至关重要。尤为重要的是要小心那些常常被低估的危险领域，例如未加密的 USB 设备、使用电子邮件发送未加密的附件，以及泄露敏感用户数据的网络浏览器。面对如此多的联网设备和不断变化的工作模式，确保手机中存储的数据与公司服务器中存储的数据一样安全至关重要。”

双因素身份验证

对于普通组织，目前为止最好、最容易做的事情是保护自己的网络外围，这简单到只需使用密码管理器和双因素身份验证。以双因素身份验证为例，系统会提示用户在笔记本电脑上提供密码，并在密码成功提供后要求用户再提供发送到用户手机的密码。

VPN 和加密 SSD/USB 设备

VPN 越来越受中小企业的青睐。VPN 对于利用公共 WIFI 网络访问公司数据的员工最为重要。但企业必须保持谨慎，避免高估 VPN 的能力。VPN 是整体解决方案的一部分，而不是全部。企业部署 VPN 常常仅仅是为了让远程工作人员使用没有任何硬件加密的笔记本电脑或便携式电脑。几乎所有人都在自己的笔记本电脑中存储文件。如果设备遭到黑客攻击、丢失或被窃，会发生什么？加密 USB 和 SSD 设备仅比标准版本略贵一点。通过部署加密 USB 设备并为笔记本电脑安装硬件加密的 SSD，可以在很大程度上应对远程办公挑战。如果设备丢失或失窃，您大可放心，没人可以访问加密的文件。您甚至可以远程销毁丢失的 USB 设备。

“我有次遇到一名网络安全专家尝试说服某公司 CEO 采用双因素身份验证，却遇到了阻力：‘不，我们不会采用，这很麻烦，是个多余的步骤，我不需要。’不久，他们就被诈骗了 40,000 英镑。”

Rafael Bloom
@rafibloom73

Salvatore Ltd 主管

“最终，提高安全意识的最佳方法是与员工进行交流，寻找既安全又有生产效率的策略。”

Rob Allen
@Rob_A_kingston

金士顿科技公司
营销与技术服务部门主管

IT 部门能否更好地保护设备？

私有服务器与 MSP

越来越多的大型组织在加紧重新在组织内部部署自己的服务器。这意味着，他们可以完全控制自己的服务器资产，不把任何东西存储在公开可访问的云中。此外还有混合服务器解决方案，其中非敏感数据仍然存储在云中，而个人数据存储在组织内部。对于第三部门的中小企业和组织而言，部署自己的服务器可能代价过于高昂。而这正是托管服务器提供商和虚拟私有服务器发挥作用的地方。这增强了对于安全性的关注，同时不会导致您的运营成本大幅增加。

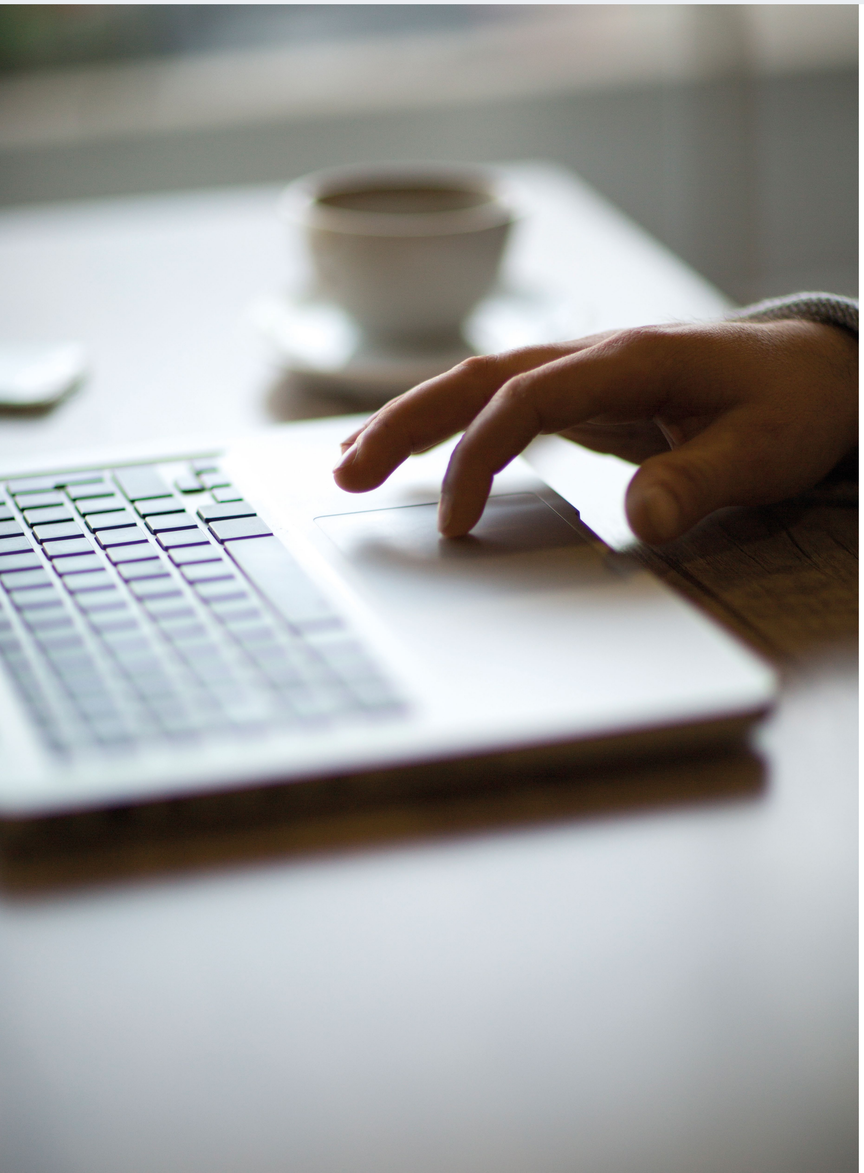
自动标记即将过期的数据

GDPR 原则之一是要求删除旧数据。例如，特定类型的个人数据的保留时间不得超过七年。如果您在数据即将过期时自动收到提示，那会怎样？利用正确的数据库，您的 IT 团队可以轻松创建一项操作，在数据接近保留截止期时向数据保护官发送一封自动生成的电子邮件。

与正确的供应商合作

在 IT 安全领域，存在无数的制造商和供应商。您应做好调研。关键在于部署来自可靠提供商的系统，这些提供商具备特定专业知识，能够在您的行业或领域为您赋能。确保您选择的供应商不仅拥有技术，还理解您在数据安全方面遇到的系统应用挑战。

第 4 章 – 技术提供商如何改善流程和理解?



数据保护官成新宠

2016 年以来市场对于数据保护官 (DPO) 的需求激增，增幅超过 700%[1]。现在，整个欧洲在职的数据保护官超过 500,000 名，为 2017 年时预期数量的六倍[2]。然而，数据保护官岗位的重要性常常被忽视和贬低。

数据保护官需要全面了解公司的安全性和数据隐私状况。这是一份全职工作。而在某些组织中，数据保护官只是最懂技术的员工的一个称号。他们对整个公司的数据隐私负责，同时履行正职的日常工作。

现实是，公司需要一系列的专业服务和工具，为数据保护官这个全新职位提供支持。即便您有全职数据保护官，面对瞬息万变的数据安全状况，未来总有挑战需要考虑他人意见。与外部咨询公司或法律顾问合作将大有帮助，但首先您必须让内部工作井然有序。

明晰、应急与融合

您的 IT 基础设施有多强大完全取决于它最薄弱的环节。因此，对于您的 IT 生态系统新增的任何因素，您的技术提供商应让您全面了解潜在安全威胁，并针对如何安全使用您的新产品提供明确建议。

Tara Taubman-Bassirian
@clarinette02

GDPR、数据保护与知识产权顾问

“我们尝试向到处安装闭路电视摄像机的人解释，这不一定安全，因为安装的摄像机常常没有密码。因此，您只需登录网站，就能看到监控的内容。这实际上是告诉盗贼:
‘趁我不在的时候来吧！”

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways www.varonis.com/blog/gdpr-effect-review/ [于 2019 年 11 月 26 日访问]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [于 2019 年 11 月 26 日访问]

技术提供商如何改善流程和理解?

接下来是应急问题。当产品使用寿命结束或需要更新时，会发生什么？针对产品无意中令产品中存储的数据陷入危险中或令您更广泛的 IT 生态系统的安全性受到威胁，技术提供商应提供应急建议。以磁共振成像扫描仪为例。它可能自带 4TB 加密 SSD，用于存储患者影像。但是，如果存储空间用尽，会发生什么？

无论是在组织内部还是与外部供应商及合作伙伴合作时，技术提供商和组织自己还必须促成数字融合和数据融合的环境。这对于英国国民保健系统 (NHS) 等多元化、多部门、多地点的组织尤其重要。

水平扫描

技术发展日新月异，有时发展步伐超过安全能力。随着新兴技术的出现，例如中国国内的面部识别支付，有时候组织会争相向市场推出技术，而没有事先考虑潜在安全和数据保护影响。5G 网络一两年内就会广泛普及，届时边缘计算和分布式数据筒仓将变成现实。技术提供商必须能够帮助组织安全地从新兴技术获益，同时不影响组织自己的数据完整性或 IT 安全。

Miriam Brown
@Kingston_MBrown

金士顿科技公司
B2B 策略营销经理

“我们向 NHS 销售了大量产品 - 但是，当我们询问他们部署了什么数据保护政策和协议时，各个信托之间存在明显差别。”

Sally Eaves
@sallyeaves

Sally Eaves Consultancy
CEO、主管

“我相信，我们将开始看到 GDPR 工作从减少实施痛点转变为专注于拓展优势，例如增强 IT 流程、备份与恢复和增强的安全性，以及将这些作为与业内同行区分开来的差异化优势。”

总结

GDPR 让企业变得更好，让数据隐私和网络安全引起公司高层管理人员和消费者的注意。不过，合规需要您的全体员工日复一日地持续关注数据安全。面对不断演变的技术和网络威胁，良好的安全基础设施和良好的培训以及技术和隐私方面的良好咨询支持，可以说对于企业至关重要。提醒员工数据背后总有人存在，这将非常有助于在您的员工中形成数据保护文化。文化变革远比打勾培训练习效果好。

关于金士顿

凭借 32 年的丰富经验，金士顿积累了发现和应对远程办公挑战的知识，让您的员工可以在任何地方安全、轻松地办公，同时不会让您的组织陷入危险之中。

#KingstonIsWithYou