参考 PCI 最佳实践合规 GDPR 个人数据保护

作者：白海蔚、刘岩（atsec 中国）

2017 年 11 月

关键词：数据保护、GDPR、PCI

atsec(Beijing) information technology Co., Ltd

Floor 3, Block C, Building 1, Boya C-Center,

Beijing University Science Park, Life Science Park

Changping District, Beijing, Postcode: 102206

P.R.China
Tel +86-10-53056681
Fax +86-10-53056678

www.atsec.cn

目录

1 GDPR 和 PCI DSS 的概念

1.1 什么是 GDPR

一般数据保护法规（GDPR：General Data Protection Regulation）（Regulation （EU） 2016/679）于 2016 年 4 月 27 日由欧洲议会（European Parliament）、欧洲联盟理事会和欧洲委员会正式发布，该法规旨在加强和统一欧盟个人的数据保护。 该法规发布同时也废除了早先发布且长期执行的第 95/46 号指令（一般数据保护法规）。

GDPR 经过两年的过渡期后，自 2018 年 5 月 25 日起成为强制执行法规。与之前发布的指令不同，它不要求各国政府通过任何授权立法，因此具有直接约束力和适用性。

GDPR 定义了处理个人数据和敏感个人数据的新规则，并定义数据存储、处理和传输的方式，这也是本文探讨 GDPR 结合 PCI DSS 标准对持卡人数据在数据存储、处理和传输的方式的意义，GDPR 法规和 PCI DSS 标准均旨在对数据在存储、处理和传输的保护。

此外，GDPR 还定义了个人对其数据如何处理的新权利，以及数据获取、存储和传播等管理方式。

该法规当前版本涉及 99 个主要条款，目前官方提供 23 种不同的语言版本。

1.2 GDPR 的背景

大数据的飞速发展，使得不论是私人公司还是跨国机构都对数据的收集和共享有了越来越多的需求，但这无疑也增加了数据泄露的安全风险。各种门户网站会员注册、APP 应用的安装使用在给广大消费者带来生活便利的同时，也使得个人数据的披露成为现代生活的一部分，每个人都对所提供的个人数据感到担忧，因为无法对所提供的数据进行任何的控制。而个人数据在不同国家有着不同的保护要求和水平，甚至因为数据不能在合理的范围内自由流动也给诸多的跨国企业在业务发展层面带来阻碍。

一直以来，欧盟在数据保护框架方面的工作较为完善，包括诸多的指令、协议和法规条例等，其中数据保护指令（正式指令 95/46 / EC）[1995]为欧盟成员国立法保护个人数据设定了最低标准。但是，随着全球范围内包括但不限于大数据、云计算、移动互联网以及各种智能终端的新技术发展，各种个人数据的存在越来越复杂，欧盟现有的数据保护条例和措施都难以适应技术发展所带来的挑战。为了应对各成员国之间对数据保护的冲突和现有措施无法应对的安全风险，GDPR 应运而生。GDPR 的发布一定程度上解决了欧洲各成员国之间由于数据保护水平不同所带来的法律失衡以及数据在各成员国之间自由流动的保护问题。

1.3 什么是 PCI DSS

PCI DSS（Payment Card Industry Data Security Standard）支付卡产业数据安全标准是一个被开发支持和提高持卡人数据安全和卡组织采用的全球化一致性的数据安全措施。提供了一套保护持卡人数据的技术和操作的基线要求。该标准由 PCI 安全标准委员会（PCI SSC：Payment Card Industry Security Standards Council）维护和推广。

PCI SSC 是由美国运通（American Express）、美国发现金融服务（Discover Financial Services）、JCB、万事达（MasterCard Worldwide）和 Visa 国际组织五家支付品牌在 2006 年秋共同筹办设立的统一且专业的信息安全标准委员会。

1.4 PCI DSS 的背景

每个拥有支付卡（包括信用卡和储蓄卡）的消费者都是持卡人。发卡机构和收单机构，在国内主要以银行为主，在国际上也有独立开展收单业务的公司。商户，例如：电子商务、大型超市、航空公司、酒店等等。首先作为持卡人（消费者），到商户进行消费，持卡人的卡数据通过网络传送给收单机构，收单机构要通过国际卡品牌的网络把数据传输给卡片的发卡机构去确认，确认后再通过卡品牌的网络回复给收单机构，收单机构将得到的确认信息通知给商户，以此完成支付的授权流程。最终商户完成这笔交易，把货品交给消费者，也从收单机构处获得货款，而持卡人接到发卡机构的账单完成还款，以此完成清算和结算。整个的消费支付过程也就包括了清算、结算和授权。上述流程即是目前支付卡交易的简要描述，而伴随近年来网上交易的增加，支付卡用卡安全问题备受关注。诸多信用卡收单机构和发卡机构、商户，以及支付服务提供商如何对支付卡数据的传输、处理和存储进行有效的保护，成为 PCI DSS（Payment Card Industry Data Security Standard）标准的主要目的。在我国国内，服务提供商的 PCI DSS 合规评估工作已经比较广泛的被接受和认可；国内银行的信用卡收单机构和发卡机构的 PCI DSS 合规建设也在近两年得到了越来越多的关注。

MasterCard、VISA、American Express、Discovery 和 JCB 是目前 PCI 产业中的五个卡品牌。每个卡品牌都有自己的安全要求，每个卡品牌所维护的安全策略体系也依然在用。2006 年，经五个卡品牌协商，为了更好的促进支付卡产业数据安全的发展，把数据保护的相关要求统一维护，成立 PCI SSC 安全标准委员会。在数据保护层面，五个卡品牌统一认可 PCI DSS 认证通过后的合规报告结果。PCI SSC 主要负责全球范围内对于数据保护标准的制定和更新、体系的管理、人员和机构的培训、审核机构的授权还有安全意识的教育等等。

1.5 GDPR 和 PCI DSS 的关系和影响

在欧盟各成员国间，GDPR 是对一般数据在传输、处理和存储的方式上规定的基本法律，目前直接适用于所有成员国，英国除外。

GDPR 规定了数据控制方、数据主体、各数据处理服务提供方、监管机构等之间数据的转移以及在发生数据泄露时的通知机制、时限和对数据的决定权等。对数据的控制和保护、程序的执行和操作也都是 GDPR 带来的直接影响。尤其是在近些年云计算的广泛应用和普及，对数据的控制力降低所带来的潜在风险，也通过 GDPR 让数据主体对数据拥有更多的控制和保护。

在业务发展层面，尤其是面向众多的全球化发展企业，早先为了顺应各个国家之间对数据保护的策略和要求，极大地增加了运营的成本。而 GDPR 的实施和生效，使企业在数据处理时形成一站式监管，打破欧盟各成员国内部的贸易壁垒，有效的降低了企业的运营成本。

GDPR 适用于数据主体在欧盟境内以及在欧盟境内向数据主体提供产品或服务的数据处理活动的企业，即使数据的控制者不在欧盟境内。据此适用性，部分中国企业必然受到此法规的约束，须遵从 GDPR 的相关要求，否则将面临高额罚款（参见本文第四章：未合规的惩罚）。

而在支付卡产业谈及数据安全保护，从合规标准的发展历史和背景来看也和 GDPR 的来源有着异曲同工之处。五个国际支付卡品牌早期各自维护的安全策略体系略有差异，这导致任何将要与多家卡品牌合作的机构需要分别且重复的通过审核从而满足业务合作层面对数据的保护要求。于是后期经五个卡品牌协商，为了更好的促进支付卡产业数据安全的发展，把数据保护的相关要求统一维护，成立 PCI SSC 安全标准委员会。并在数据保护层面，统一认可 PCI DSS 认证通过后的合规报告结果。

目前在中国大陆地区，服务提供商的 PCI DSS 合规评估工作已经比较广泛的被接受和认可，国内银行的信用卡收单机构和发卡机构的 PCI DSS 合规建设也在近两年得到了越来越多的关注，VISA、万事达等作为卡组织，其风险管理的要求中对于收单和发卡机构的 PCI DSS 合规建设也是重中之重。而互联网、大数据等新技术高速发展下伴随而来的数据泄露问题，使得对数据保护的范围需求扩大。诸多的参与支付环节的行业机构均纷纷通过了 atsec 中立的基于 PCI DSS 的合规评估。例如，航空公司除了担心直接与支付交易相关的系统安全性建设以外，开始关注常旅客信息的保护；大型酒店除了担心资金的损失、账户的安全性以外，开始关注会员注册个人信息的保护。经过 PCI DSS 标准多年来对支付卡数据实施落地的保护措施，越来越多的机构采用 PCI DSS 标准作为对数据传输、处理和存储方式保护的基本要求。且经过对 GDPR 法规和 PCI DSS 标准对比不难看出，如果已经合规了 PCI DSS，可以处理所有的其它数据采用和 PCI 标准要求同样的保护措施通常就可以达到 GDPR。

而在 GDPR 和 PCI DSS 所涉及的产业角色中也可达到一定的对应和关联：

- GDPR 定义的数据主体类似于支付产业链中的持卡人，是提供数据的一方；
- GDPR 定义的数据控制方，被批准进行数据收集的机构，类似于支付产业链中的商户收集支付卡数据；
- GDPR 定义的数据处理方，为控制方提供需要的任何活动。例如 Web 托管提供程序是数据处理而不是数据控制，类似于 PCI 中支付产业链中的服务提供商。

PCI DSS 是技术性的标准，为合规体系的构建提出了技术的规范根基。GDPR 是法规层面的要求，从更加宏观更加广泛，以及更加严格的要求层面提出了基本的针对个人数据的保护规定，实施过程中结合技术层面的最佳实践，如 PCI DSS 将为机构的合规起到积极和推动的作用。

2 数据的定义和分类

通常情况下 GDPR 一般数据保护法规中将数据分为数据和敏感数据。所提及的数据指相关个人数据涉及的是一种生活中可识别的个人数据，包括对个人的任何意见表达以及对个人意图的任何表示，还有姓名、地址等；以及信用卡号码。

敏感的个人数据组成的数据信息包括但不限于：

- 数据主体的种族或族裔来源；
- 政治观点；
- 宗教信仰或类似性质的其他信仰；
- 他是否是工会会员；
- 身体或精神健康或状况；
- 性生活；
- 犯罪行为或者涉嫌的犯罪；
- 等等。

同样的，PCI DSS 标准针对要保护的数据也分为持卡人数据和敏感的验证数据，所包含的数据信息参见下表：

	数据元素	允许存储	按照要求 3.4 实现存储数据的不可读性
持卡人数据	主帐户 (PAN)	是	是
	持卡人姓名	是	否
	业务码	是	否
	失效日	是	否
敏感验证数据 [2]	全磁道数据 [3]	否	要求 3.2 规定不能存储
	CAV2/CVC2/CVV2/CID[4]	否	要求 3.2 规定不能存储
	PIN/PIN 数据块 [5]	否	要求 3.2 规定不能存储

不难理解，当我们需要针对数据或者敏感数据在进行传输、处理或存储过程中进行保护时，我们可依照 PCI DSS 标准中对持卡人数据和敏感验证数据的保护措施进行。我们将个人数据视为持卡人数据，而敏感的个人数据视为支付卡产业的敏感的验证数据。

数据的收集需要被机构进行合理的评估：

- 确定什么数据需要收集及其原因；
- 不要收集你不需要的数据；
- 将数据进行分类：
  - 个人数据；
  - 敏感个人数据。

我们可以考虑将个人数据视为 PCI 产业内的持卡人数据进行保护，而将敏感的个人数据视为敏感的验证数据进行保护。

3 GDPR 法规的义务和个人的权利

3.1 GDPR 法规的义务

GDPR 法规明确了数据控制方和数据处理方在数据活动处理时需综合考虑数据处理的性质、范围和目的，且需要对数据主体进行监控，同时要求设置数据保护专业人员，以到达监管、行使权利和各方沟通的目的。

GDRP 法规明确了对于发生数据泄露事件时的通知机制，包括与监管机构之间的汇报、与数据主体之间的影响以及个人需要采取的及时措施通告等等。

GDPR 法规明确了一般数据在欧盟各成员国之间传输的规则，在何种情况下禁止发生数据传输，例如需要接收数据的一方无法确保接收数据的安全性。

GDPR 中定义的数据控制方需要确保个人数据满足如下条件：

- 合法、公平、透明的处理与个人有关的问题；
- 有特定的、明确的和合法的目的而需要收集的数据，说明所处理有关数据的必要性、充分性以及相关性和有限性；
- 准确且是最新的（如果必要）；
- 保存的形式能允许数据主体识别不必要的个人数据；
- 处理的方式能够确保合适的个人数据安全。

此外，还需要考虑如下技术机制，如数据加密、访问控制、数据保留、TLS 1.2 的安全性问题、日志等。

更多 GDPR 法规提及的各方义务请参考法规原文，本文仅举例说明。

而 PCI 支付产业链与 GDPR 法规规范的各方义务所提出的一些逻辑也是十分相似的。在整个支付流程中通常涉及发卡机构、收单机构、服务提供商、终端机具厂商、支付应用软件开发商、商户、持卡人，当各方之间因为业务需要产生合作时，将会发生数据的传输和协同处理工作，而每一个角色在确保进行自身数据安全合规建设的同时，则需要确保合作的上游或者下游企业具有同样水平的数据保护措施，从而达到整个产业或者生态的数据安全。

3.2 个人的权利

GDPR 法规也同时规定了对于个人的权利，个人作为用户必须明确：

- 同意数据控制方收集所需的数据；
- 在 GDPR 框架体系下，要求下明确肯定的同意；如果是隐藏（沉默）、预选择的或者不是主动确认的同意，则不能构成个人的同意；
- 同意提供的数据必须是可被核查的，意味着一些数据会被保存，并以某种形式或某个时间得到同意；
- 个人有权随时撤回同意；
- 可以依靠其他法律基础来同意。例如，为了你的组织或第三方的合法利益，加工是必要的；
- 日志、记录保持、数据保留。

GDPR 法规也给个人提供以下权利：

- 知情权；
- 获取或访问权；
- 矫正权；
- 删除权；
- 限制处理权；
- 数据可移植的权力；
- 反对的权利；

- 与自动决策和分析有关的权利。

针对所有受影响方实施、更新和已知的可重复性的过程，需要进行书面文档化，并在规定的时间或被要求时执行数据的删除。

4 未合规的惩罚

GDPR 规定了欧盟内各成员国均须成立关于 GDPR 的监管机构（“Supervisory Authority”）负责 GDPR 的执行并接受本国内的违法投诉，同时负责与欧盟其他成员国监管机构进行沟通以保证在同一事件上执法力度统一。监管机构有权对疑似的违法事件进行调查，并根据调查结果进行相应的处罚。

根据本文上述内容所介绍，欧洲议会通过的 GDPR 一般数据保护法规将在 2018 年 5 月 25 日生效。对于在欧盟任一成员国内有分支机构的中国企业，所在地的分支机构将被视为责任主体被强制要求执行该法规。非欧盟成员国的企业若达到以下两种情况之一，则同样受到 GDPR 限制：

- 为欧盟各成员国范围内可识别的自然人提供商品和服务而需要收集、处理个人信息；
- 为欧盟各成员国范围内可识别的自然人的活动而需要收集、处理个人信息。

故而该法规将对中国企业的移动应用安全，以及数据收集、处理和交易带来重大影响。

根据 GDPR 法规要求，管辖范围内（由于英国已退出欧盟，所以不包含在此范围内）的企业如果未能合规，则会面临潜在的罚则，罚则标准如下：

- 一般违规罚款的上限是 1000 万欧元或该企业上一财年全球年度营业总额的 2%（以较高者为准）（参见法规第 83 条第四段）；
- 严重违规罚款的上限是 2000 万欧元或该企业上一财年全球年度营业总额的 4%（以较高者为准）（参见法规第 83 条第五和六段）。

PCI 产业对于疑似数据泄露事件的事后取证和调查流程与 GDPR 一般数据保护法规所要求设置的监管机构职责和管理方法非常类似。PCI SSC 在全球范围内授权 PFI（PFI：PCI Forensic Investigators）取证调研机构，当发生疑似数据泄露事件后，卡组织将联合发卡机构、收单机构以及有资质的 PFI 取证机构对事件进行取证分析，并出具 PFI 报告，而后续各责任方也将基于该取证报告进一步判定罚则。atsec 即是被授权在中国地区执行 PFI 取证调研实验室。但我们仍然希望各企业重视数据安全保护工作，协助各企业在事前进行合规建设，以免遭受处罚给企业声誉和资金等方面带来损失。

5 atsec 可以提供的服务

在支付产业的整个合规体系中 PCI DSS 是面向整个支付流程所涉及的持卡人数据环境范围的审核，在这个大的环境范围当中涉及到支付应用软件、支付终端类硬件产品，实际上都有对应适用的标准。支付卡产业链的安全标准包括 PCI DSS ，PA DSS，PTS， P2PE 以及面向卡厂的逻辑和物理安全标准等。每个安全标准均由 PCI SSC 授权独立的审核机构。

atsec 是针对支付卡产业数据安全标准（PCI DSS：Payment Card Industry Data Security Standard）授权的合格安全评估机构（QSA：Qualified Security Assessor）和授权扫描服务商（ASV：Approved Scanning Vendor），以及支付应用合格安全评估机构（PA QSA：Payment Application Qualified Security Assessor）和 PCI 取证调研 PFI 机构（PFI：PCI Forensic Investigators）和 P2PE（PA）审核机构。

atsec 作为 PCI DSS QSA 审核机构，基于 PCI DSS 标准在应用与数据管理层面、软件生命周期层面、漏洞管理与信息安全层面、系统组件运维与物理安全层面和参考产业的最佳实践领域展开对数据保护安全合规建设。而 QSA 可能在一次评估审核时无意中接收到个人数据，例如流量捕获中对于交易的详细信息、在数据库传输或者日志中记录的消费者详细信息、个人数据截图等，而 QSA 必须确保这些数据是安全的。

PCI DSS 为 GDPR 要求的个人数据管理提供了一个很好的框架，如果基于 PCI DSS 标准，可以采用 PCI DSS 标准要求的保护措施以同样的方式对待所有的一般数据。 虽然 PCI DSS 并没有涵盖 GDPR 要求的所有内容，但是缺少的元素很容易实现，可以通过 PCI 标准的扩展或使用其他标准要求来实现。 这里简要分享 PCI DSS 标准要求框架如下：

建立和维护安全的网络 Build and Maintain a Secure Network and Systems	1. 安装并维护防火墙配置以保护持卡人数据 Install and maintain a firewall configuration to protect cardholder data 2. 系统口令和其它安全参数不使用厂商默认设置 Do not use vendor-supplied defaults for system passwords and other security parameters
保护持卡人数据 Protect Cardholder Data	3. 保护存储的持卡人数据 Protect stored cardholder data 4. 对公共开放网络上传输的持卡人数据加密 Encrypt transmission of cardholder data across open, public networks
维护漏洞管理程序 Maintain a Vulnerability Management Program	5. 使用并定期更新防病毒软件 Protect all systems against malware and regularly update anti-virus software or programs 6. 开发和维护安全的系统和应用 Develop and maintain secure systems and applications
实施访问控制措施 Implement Strong Access Control Measures	7. 限制对持卡人数据的访问到必需的业务访问 Restrict access to cardholder data by business need to know 8. 对计算机访问用户分配唯一的帐号Identify and authenticate access to system components 9. 限制对持卡人数据的物理访问 Restrict physical access to cardholder data
定期监控和测试网络 Regularly Monitor and Test Networks	10. 跟踪并监控对网络资源和持卡人数据的所有访问 Track and monitor all access to network resources and cardholder data 11. 定期测试安全系统和流程 Regularly test security systems and processes
维护信息安全策略 Maintain an Information Security Policy	12. 维护信息安全策略，以解决内外部的安全问题 Maintain a policy that addresses information security for all personnel

PCI DSS 标准从信息安全管理体系、网络安全、物理安全、数据加密等方方面面提出了诸多的安全基线要求。虽然没有任何一个信息安全标准或者安全建设可以保障实现百分之百的抵御安全风险，然而根据业界的积累，能够实现 PCI DSS 并且严格按照 PCI DSS 的要求持续实施针对持卡人数据环境的安全防护，数据泄露的安全事件发生的可能性将大大降低。

除了很多具体的技术改进和安全防护提高之外，致力于 PCI DSS 合规建设评估工作的价值大体可以总结为以下几个层面：

- 识别和发现机构可能被攻击的薄弱环节；
- 通过外部独立的第三方评估机构的安全评估提高机构自身的安全级别和降低安全风险；
- 提高人员信息安全意识；
- 管理体系的符合性建设可以塑造良好的机构经营形象，正式评估结果更进一步验证并公开认可其符合性；
- 增强与业务往来伙伴的信心和满意度；
- 管理体系的建设进一步加强机构的内部管理和控制；
- 可以降低诸多的成本和费用；
- 符合性建设和认证具有市场价值，在同行业同领域对手面前占据绝对的优势，提高自身竞争力；
- 符合性建设和认证可以为全球信息交流建立国际信任且认可的平台，是机构在世界舞台上展现自己的重要因素，也很有可能是先决条件。

PCI DSS 的实施方案不仅在面向支付产业链上所有机构对持卡人数据进行有效保护，也可以借鉴并扩展到满足 GDPR 法规对一般数据的保护中。需要所有涉及到数据（不论支付卡数据还是一般个人数据）的存储、处理和传输的各个机构的共同参与，只有全面广泛的实现了合规才能真正做到保护数据降低数据泄漏的风险。

6 参考文献

[1]. GDPR: http://www.consilium.europa.eu/

[2]. Directive 95/46/EC: http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:31995L0046

[3]. EUGDPR.org: https://www.eugdpr.org/

[4]. atsec: http://www.atsec.com