美国安全港法规

欧盟的综合隐私法规——隐私数据保护法案（简称欧盟隐私法案）--在1998.10.25生效。该法案要求仅在向非欧盟构架传输个人数据时要求提供足够的隐私保护等级。

尽管美国和欧盟都致力于增强对公民隐私的保护这一共同的目标，但美国采用不同于欧盟的方法保护隐私。美国使用基于多个法律、法规和自愿（self regulation）的方法。由于这些差别，许多美国组织反映不确定欧盟所说的“足够的标准”对于从欧盟传至美国的个人数据有何影响。

为了减少这种数据传输的不确定性并提供更可预期的框架，1998年11月4日，美国商务部发布了《国际安全港隐私保护原则》和FAQ（简称“安全港法规”，或在不会引起混淆的情况下，简称“法规”）以培育、推广和开发国际商业。安全港法规经咨询工业界和大众而制定以加速欧美之间的贸易和商业。仅适用于美国组织，当其从欧盟收到个人数据时，确保安全港和“足够”保护的假设。因为规范仅为了达成这个特定的目标而制定，应用于其他目的可能（may）不恰当。安全港法规不能用作各洲制定的欧盟隐私法案的用于个人数据处理的实施方案。

安全港是指某一特定的在线服务商应公布产业的网络隐私保护的行为指引，该指引由联邦贸易委员会通过后，即成为个人隐私信息的“安全港”，网络服务商只要遵守该指引，就可以被认为是遵守了保护个人数据的有关要求。

各组织确实执行安全港法规的决定完全取决于自愿，并且各组织执行安全港法规的方法可能各异。决定依循安全港法规的各组织必须遵从法规以达到获得和保持安全港的益处并且公开宣布他们将如此做。例如，如果一个组织参加一个自治的隐私项目依循安全港法规，他作安全港达标。各组织亦可通过开发他们自己的自治隐私策略与法规一致而达标。当与法规一致时，这个组织完全或部分的依赖自治，若未能自治，该组织（见附录美国为欧盟认可的组织）受联邦贸易委员会（ FTC ）法规（第五章禁止不公平和欺骗的行为）或者其他法律法规（禁止此类行为）的惩罚。另外，遵循法规、管理条例、或其它法律（或原则）的各组织也可遵守安全港法规。期望做安全港认证的每个组织自发证书至商务部（或其指定单位）说明其遵守法规，自发证书指南见FAQ自发证书部分，在各种情况下，自各组织的自发证书签发即日起，必须确保安全港利益。

与法规的一致性可能有如下限制：（a）限于满足国家安全、公共利益或者法律强制要求的范围；（b）限于法令、政府法规、案例法律与其冲突的强制要求或明显的权威性，假设如此，各组织在实施这些权威规定时可声明其与法规不一致的点限于超越其上的法律利益；（c）限于欧盟隐私法案或者各洲法律允许的例外或违背，假设这种例外和违背应用在可比较的前后文。为了与保护隐私的目标一致，各组织需（Should）为了完全和透明的实现法规而努力，一般做法包括指出他们的隐私策略，说明例外的是（b）所述法律。为了同样的原因，如果遵守法规和/或美国法律可选，可能的话，期望各组织倾向于遵守更高的保护措施。

各组织可能期望为了实施或其他原因而在所有数据处理中均使用法规，但是各组织仅被强制要求在数据传入安全港后应用法规。为了安全港认证，各组织未被强制要求在手工处理的文件系统中应用法规。期望获得安全港益处的各组织对于手工处理文件系统信息从欧盟传入安全港后，必须应用法规。——某个组织若期望将安全港益处扩展至来自欧盟的用于招聘的人力资源个人信息，当其向商务部（或其指定单位）自签证书的时候，必须指出这一点，并且依照 FAQ 中关于自签发证书的需求去做。各组织如果在和合作伙伴的书面合同中包含安全港法规，其也愿（will）提供欧盟隐私法案第 26 章要求的必要的保护措施，作为从 EU 传输数据的实际的隐私条款（provision），一旦在此类模型合同的其他条款经 FTC 和成员州授权。

个人数据或个人信息是欧盟隐私法案内定义的个人标识数据，由美国组织自欧盟接收并以各种形式存储。

安全港规定的主要内容项：

1）通知：一个组织必须通知个人其搜集和使用个人信息的目的，怎样联系这个组织以咨询或投诉，其将透露（disclose）数据给哪些第三方，个人对于个人信息限制使用或透露的选项和方法。当组织第一次要求用户提供个人信息之前或者第一次非原目的使用个人信息或者第一次透露给一个第三方之前，必须以清楚、鲜明的语言通知用户。

2）选择：一个组织必须提供给个人选择是否（默认是）他们的个人信息（a）可透露给第三方，或（b）可使用于与（搜集和数据授权的）原目的不相容的目的。一个组织必须提供给用户清楚、鲜明、可达、可支付得起的机制作选择。

对于敏感信息（即关于医疗、健康状况、民族和种族的起源、政治观点、宗教和哲学信仰、商业联盟的成员、私生活的信息），必须以证实或显式的选项提供给用户是否（默认否）可透露给第三方或者使用于和原目的不相容的目的。任何情况下，一个组织必须将从第三方收到数据作为敏感数据处理，如果第三方将该数据处理并标识成敏感数据。

3）前转：透露给第三方的信息各组织必须应用通知和选择原则。当一个组织期望传输数据给第三方时，如该组织的一个代理（如尾注所述），可(may)这样作：如果该组织第一次确定第三方遵从安全港法规、或者遵从欧洲隐私法案、或者另一个足证、或者在书面合同中写明第三方提供安全港法规要求的同等的隐私保护措施。如果该组织遵从了这些需求，其不必（shall not）对接收数据的第三方（除非该组织承认）违反任何限制或条款处理个人信息一事负责，除非该组织已知或应已知该第三方将违规，但是该组织未采取任何合理的行为预防或阻止这样的处理。

4）**安全：**各组织创建、维护、使用或分发个人信息必须采取合理的预防措施以保护数据，使其不丢失、误用和未经授权的访问、透露、变更和破坏。

5）**数据完整性：**与安全港法规一致，个人信息必须与其要使用的目的一致。一个组织不能（may not）为了与信息搜集或个人授权的原目的不相容的目的对个人信息进行处理。为确保原目标，一个组织应该（should）采取恰当的步骤保证这些数据在使用方式、准确性、完整性和实时性是可信赖的。

6）**强制执行：**有效的隐私保护必须包括确保本法规被遵从的机制，当个人数据被违规处理时当事人的求助机制以及当组织不遵守本法规的的后果。最低限度的，这些机制必须包括 a）一个现成可用并可支付得起的独立求助机制，通过该机制，个人的投诉和争论可被调查并参考本法规解决，并根据适用的法律或其它隐私章节的规定对损失进行赔偿。b)验证商业组织声明的隐私策略的真实性，以及隐私策略是否如实执行的追踪过程。c)对由因为组织不遵从本规范而引发的问题，通过公布其与这些问题的关联和可能造成的后果，敦促其履行纠正的义务。制裁必须足够严厉以确保各组织遵从本法规。

注：当第三方是某组织的代理，其代表该组织或在组织指导下执行任务时，

该组织传输信息给此第三方时，不需要提供通知或者选择措施。另一方面，前转规则不适用于这种透露。