SANS SECURITY AWARENESS

給大家的安全意识通讯月刊

GDPR《一般数据保护条例》

概述

你可能听说过一个新的法律条文称为GDPR，或《一般数据保护条例》. 这项法律是由欧洲联盟制定的，并於2018年5月25日生效. 它适用于任何组织须要处理《欧洲联盟》(简称欧盟) 内任何居民的个人讯息，无论該组织位于世界那一个角落。 GDPR要求组织维护任何欧盟居民个人讯息的隐私和安全性。 为了确保遵守GDPR的要求，这必须要确定关键原则来理解和落实。

人们有权去享有隐私权。 通过限制他们收集和处理个人资料并通过维护这些数据的大前提下，组织必须尊重他们所拥有的隐私权。 通常来说，我们的隐私义务适用于任何讯息，包括讯息本身以及能通过其识别到个人的其它相关讯息，目的是为了确定可以个人身份生活在欧洲联盟内。 这些讯息可以是联系地址、护照号码、驾照号码、财务讯息、生物识别特征、协会会员、病史、位置讯息或者有关个人性取向、宗教或政治信仰的讯息。 法规适用于每个“自然人”，这是指每一个个体。 以下是GDPR中必须遵守的主要原则:

- 當事人的个人资料应依法、公平和透明地处理。
- 人们需要被告知在收集甚么和是甚么样的目的。
- 个人资料收集应为是指定的、明确的和目的是合法的。 这个不得用于任何与上述目的而相抵触，这会与其他理由产生冲突。
- 个人数据应该只保存和处理那一些必要用的，其他可以不用理会。

必须维持最新和准确的个人数据。

人们有权拿取他们的数据副本，或者要求他们的个人数据不会再使用，或者在某情况下完全删除。

组织机构必须执行相应的安全措施来保护个人讯息，避免其遭到意外或非法破坏、丢失、篡改和泄露。

此外，组织必须要确保处理个人数据的所有工作人员，在如何保护个人讯息和数据保护方面受过适当的培训。

为保障个人资料所实施的保护措施，必须保证那保护级别与讯息的敏感级别相符。 若与数据相关风险增加，那么在保护数据措施上花费的精力以及费用也随之提升。 必须按时定期审查和更新这些措施。 保存良好的隐私安全决策及措施的记录，证明了我们充分地遵守法规条例的要求。 此外，我们依法采取包括合约和尽职审查评估在内的措施，在向外包人员或欧盟外第三方成员转移个人讯息时能保障隐私安全。 最后，若意识到个人数据违约这一点底下，组织应在知悉后72小时内报告违规的情况。 如果组织不遵守 GDPR《一般数据保护条例》 就会导致罚款高达全球收入的 4%，使 GDPR《一般数据保护条例》 成为全球世界经济上代价高昂的法规之一

特邀编辑

布赖恩. 河楠 是"BH咨询服务的总经理"， 一个驻在爱尔兰都柏林的独立咨询网络安全与数据保护的供应商。 布赖恩曾担任《欧洲刑警组织内网络犯罪中心》的特别顾问简称(EC3)， 是爱尔兰国家第一个取得证书的创办人，他亦在多家创新型安全公司担任咨询委员会。 寻找布赖恩请登上 www.linkedin.com/in/brianhonan 或 Twitter @brianhonan.

参考资料

GDPR《一般数据保护条例》 个人和组织的概述: http://gdprandyou.ie
GDPR《一般数据保护条例》法规: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679
OUCH! 翻译和档案: https://www.sans.org/u/D88