TC260-PG-20183A

网络安全实践指南

—欧盟 GDPR 关注点

v1.0-20180525

全国信息安全标准化技术委员会秘书处

2018 年 5 月 25 日

本文档可从以下网址获得：
www.tc260.org.cn/

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全实践指南》（以下简称“实践指南”）是全国信息安全标准化技术委员会（以下简称“信安标委”，TC260）发布的技术文件。实践指南旨在推广网络安全标准，应对网络安全事件，改善网络安全状况，提高网络安全意识。

声　明

技术支持单位

本实践指南得到中国电子技术标准化研究院、北京大学、腾讯、蚂蚁金服、京东、高德、华为、微软、百度、甲骨文、戴姆勒等单位的技术支持。

摘　要

本实践指南简要介绍GDPR适用的场景、核心内容和关注点，仅供参考，旨在提示读者关注GDPR实施对其产生的影响。

关键词：GDPR；个人数据；风险管理；关注点

2018年5月25日，欧盟通用数据保护条例（General Data Protection Regulation，GDPR）正式实施，在全球范围内产生广泛影响。相关组织在符合我国个人信息保护相关规定的基础上，随着业务和合作范围的不断扩大，建议就其部分可能涉及的场景，密切关注国际上数据保护的相关要求。

关于GDPR，建议重点关注以下几点：

关注点一：适用 GDPR 的场景

GDPR第三条规定，以下两类情形在其适用范围内：

一是数据控制者或数据处理者在欧盟境内设有分支机构（establishment）。在此情形中，只要个人数据处理活动发生在分支机构开展活动的场景中（in the context of the activities of an establishment），即使实际的数据处理活动不在欧盟境内发生，适用GDPR。

例如，在欧盟本地运营的A国（A国指某一非欧盟成员国）连锁酒店，直接将其收集的住客个人数据传输至A国总部进行处理，则需要履行GDPR中相关责任和义务。

二是数据控制者或数据处理者在欧盟境内不设分支机构（establishment）的情形。在此情形中，GDPR原则性地规定只要其面向欧盟境内的数据主体提供商品或服务（无论是否发生支付行为），或监控（monitor）欧盟境内数据主体的行为，适用GDPR。

例如，A国境内运营的某一电商平台，在欧盟不设分支机构，但提供专门

的法文、德文版本的页面，同时支持用欧元进行结算，支持向欧盟境内配送物流。该电商平台属于面向欧盟境内的数据主体提供商品或服务，需要适用GDPR。

例如，在A国运营的社交媒体平台，支持境外账户注册，且已有欧盟境内用户使用。该社交媒体平台根据用户的位置信息、浏览记录等行为信息，向用户推送个性化的信息和广告，有可能被欧盟的个人数据保护机构（Data Protection Authority）认定为监控（monitor）欧盟境内数据主体的行为，适用GDPR的可能性较高。

例如，A国企业开发的软件或系统被嵌入某款设备，该设备向欧盟地区销售，该设备的制造商在欧盟境内设立了销售代表处，相关软件或系统收集个人数据的过程需要适用GDPR。

此外，GDPR主要适用欧盟境内发生的个人数据处理行为，其保护对象为欧盟境内的数据主体。当欧盟公民抵达A国，例如进入A国大学学习，在A国商场购物等，且欧盟公民返回欧盟境内后，大学、商场不再对其行为进行跟踪或分析，则大学、商场无需适用GDPR。

组织涉及海外业务、全球化经营或业务合作等场景时，应注意其是否适用GDPR。

关注点二：适用的数据范围

GDPR规定，个人数据，是指与一个确定的或可识别的自然人相关的任何信息。可被识别的自然人,是指借助标识符，例如姓名、身份标识、位置数据、网上标识符，或借助与该个人生理、心理、基因、精神、经济、文化或社会身份特定相关的一个或多个因素，可被直接或间接识别出的个人。

GDPR规定，特殊类别（敏感）个人数据，是指揭示种

族或民族出身，政治观点、宗教或哲学信仰以及工会成员的个人数据，以及唯一识别自然人为目的的基因数据、生物特征数据、自然人的健康、性生活或性取向数据，还包括刑事定罪和犯罪相关的个人资料等。

组织应识别其处理个人数据或特殊类别（敏感）个人数据的具体类型。

关注点三：数据处理的基本原则

GDPR规定了个人数据处理的基本原则，包括合法、公正、透明、数据最小化、目的限定、存储限制、完整性和保密性、问责等;

GDPR规定，数据处理是指针对个人数据或个人数据集合的任何一个或一系列操作，诸如收集、记录、组织、建构、存储、自适应或修改、检索、咨询、使用、披露、传播或其他的利用，排列、组合、限制、删除或销毁，且无论此操作是否采用自动化的手段。

组织应保证其数据处理活动遵循基本的原则。

关注点四：数据处理的合法正当性事由

GDPR规定，数据处理行为首先应具备合法性基础，GDPR规定的六种合法性情形包括：数据主体的同意、合同履行、履行法定义务、保护个人重要利益、维护公共利益以及追求正当利益。

GDPR强调同意是指“数据主体通过书面声明或经由一

个明确的肯定性动作，表示同意对其个人数据进行处理。该意愿表达应是自由给出的（freely given）、特定具体的（specific）、知情的（informed）、清晰明确的（unambiguous）”，且撤回同意的方式应该与表达同意同等便利。

组织应保证其数据处理活动满足合法性要求。

关注点五：对儿童的特别保护规定

GDPR认为，儿童可能不太了解有关个人数据处理的风险、后果以及他们在数据处理中所拥有的权利，因此在收集有关儿童的个人数据时和将其个人数据使用在对儿童提供营销或创设个人账户的服务时，应予以特别保护。GDPR在“信息社会服务中适用儿童同意的条件”规定，如果直接向儿童提供信息社会服务时，该儿童的年龄应当为 16 周岁以上。若儿童未满 16 周岁，只有在征得监护人同意或授权的范围内其处理才合法。

组织如涉及儿童个人数据的处理，应予以特别保护。

关注点六：数据主体权利

GDPR赋予了数据主体对其数据广泛的控制权，包括知情、访问、更正、删除、限制处理、可携带、反对等权利。比如:

在数据收集时，数据控制者应以简洁、透明、易懂及便于访问的方式向数据主体提供数据控制者身份及联系信息、

数据处理的目的及合法基础、数据主体享有的权利等信息。

在特定情况下，如履行目的不再需要、数据主体撤回同意或个人数据被非法处理等等情况下，数据主体有权要求删除其个人数据。GDPR也规定了若干删除权不适用情形，如为行使言论和信息自由的权利，为履行数据控制者法定义务，为设立、行使或捍卫合法权利等等。

数据主体有权拒绝数据控制者基于以下目的对个人数据进行的处理行为，如为公共利益，为数据控制者的合法利益，以直接营销为目的，基于科学或历史研究以及统计目的的数据处理行为等。

数据主体有权在以下情形限制数据控制者的处理行为，如质疑数据准确性，违法处理，数据到期等。

数据控制者基于数据主体同意或履行合同所必须，以自动化方式处理数据主体提供的个人数据时，数据主体有权从数据控制者取得结构化可机读的个人数据副本，并传送给另一个数据控制者。

组织应基于当前业务特点及处理数据的合法性事由，选择需要实现的数据主体权利。

关注点七：对用户画像的规定

GDPR规定，用户画像是指通过自动化方式处理个人数据的活动，用于评估、分析以及预测个人的特定方面，可能包括工作表现、经济状况、位置、健康状况、个人偏

好、可信赖度或者行为表现等。如电商通过用户画像，开展广告、市场预测和推广工作。

GDPR规定，在数据主体明确同意、欧盟或者成员国法律的明确授权、履行合同所必需的情形下可以使用用户画像。同时还提出，在征得数据主体同意时，应对画像相关数据来源、算法原理及相应影响等予以充分告知，并赋予数据主体反对权、删除权、更正权和限制处理权等权利。

组织如涉及对用户进行画像，需要关注如何获得合法性基础，以及向数据主体提供相应权利。

关注点八：对数据处理者的规定

GDPR规定，数据处理者是指为数据控制者处理个人数据的自然人、法人、公共机构、行政机关或其他非法人组织。

GDPR规定，当数据控制者委托数据处理者具体处理数据时，数据控制者应选择采取了合适的技术和组织方面措施的数据处理者，以确保数据处理符合GDPR的要求，及保障数据主体的权利。在没有数据控制者事先或一般性的书面许可时，数据处理者不应再与另外的数据处理者合作。

组织如属于数据处理者，应根据数据控制者明确的指示处理个人数据，履行相应的保密义务，在数据处理服务结束时，删除或返还所有的个人数据，接受数据控制者的审计等。

关注点九：对数据保护官、欧盟境内法律代表的规定

GDPR规定，通常情况下，数据控制者和数据处理者任

命数据保护官的情形包括：（1）公权力机构处理数据的；（2）数据处理的主要活动范围、目的要求经常性、系统性、大范围地监测数据主体；（3）大规模处理特殊类别个人数据。

数据保护官应具备专业的数据保护法律和实践的知识，以保证其履行相应职责。数据保护官可以是正式职员，也可以基于服务合同完成工作。数据控制者应公开数据保护官的联系方式，并将名单向监管机构汇报。

如果组织面向欧盟境内的数据主体提供商品或服务，或监控欧盟境内数据主体的行为，应通过书面形式在欧盟境内任命一名代表。

组织如存在上述情形，应考虑设立数据保护官或任命欧盟境内法律代表。

关注点十：对数据保护影响评估的规定

数据保护影响评估（DPIA）是有助于降低数据处理风险的重要工具。DPIA分析数据处理的必要性和适当性，通过识别和评估风险并确定相应的防护措施，帮助数据控制者管理个人数据处理给自然人权利和自由带来的高风险。除此之外，DPIA也可向监管者证明其实施了GDPR中的相关要求。

GDPR规定，数据控制者在进行数据处理之前，基于数据处理的性质、范围、内容及目的判断处理活动可能对个人的权利和自由构成高风险时，应实施DPIA。在以下情形下，

通常需要实施DPIA：一是基于数据的自动化处理，包括数字画像，对自然人个人方面的系统和广泛的评估，而据此做出的决定对该自然人产生法律效力或者重大影响；二是大规模特殊类别个人数据或有关犯罪记录和违法行为的个人数据；三是对公共区域大规模的系统化监控。

组织如构成上述情形，应考虑实施数据保护影响评估（DPIA）。

关注点十一：通过设计实现数据保护的规定

GDPR规定，数据保护设计理念应当融入到产品和业务开发的早期过程（Privacy by Design），例如，设计假名化等机制有效地落实数据保护原则，并且将必要的保障措施融入到数据处理过程之中。此外，组织可实施相应的措施以确保在默认情形下，仅仅处理为实现目的而最少必需的个人数据。

组织应注意其产品和业务的设计理念与GDPR保持一致。

关注点十二：数据泄露强制通知的规定

GDPR规定，在发生个人数据泄露时，除非个人数据的泄露不会产生危及自然人权利和自由的风险，否则数据控制者应在获知泄露之时起的 72 小时内向监管机构发送通知报告。另外，当个人数据泄露可能对自然人的权利和自由产生高风险时，数据控制者还应当向数据主体告知数据泄露的相

关情况。

组织应注意如发生个人数据泄露等安全事件，需履行的通报和告知义务。

关注点十三：数据跨境传输的规定

GDPR提出了多种数据跨境流动机制。比如，直接向通过欧盟进行充分性认定的第三国传输数据，还可通过实施被认可的行为准则，签署符合相关要求的格式合同、有约束力的公司准则、通过相关认证等方式证明数据接收方满足适当的保护能力，来保证数据跨境流动的安全性；此外，在征得数据主体明示同意、基于公共利益、履行有利于数据主体的合同或基于组织正当利益等情形下也满足数据跨境传输要求。

组织如涉及数据跨境传输，应选择适用于其业务的跨境传输机制。

关注点十四：处罚规定

GDPR对违规组织采取根据情况分级处理的方法，并设定了最低一千万欧元的巨额罚款作为制裁。如果组织未按要求保护数据主体的权益、做好相关记录，或未将其违规行为通知监管机关和数据主体，或未进行数据保护影响评估或者未按照规定配合认证，或未委派数据保护官或欧盟境内代表，则可能被处以 1000 万欧元或其全球年营业额 2％（两者取其高）的罚款。

如果发生了更为严重的侵犯个人数据安全的行为，如未获得客户同意处理数据，或核心理念违反“隐私设计”要求，或违反规定将个人数据跨境传输，或违反欧盟成员国法律规定的义务等，组织有可能面临最高 2000 万欧元或组织全球年营业额的 4%（两者取其高）的巨额罚款。

组织可向其内部通报GDPR处罚规则，进一步提升安全意识。

关于欧盟 GDPR 原文，参见：

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC