

个人信息安全保护

专业课小课堂



主讲：曹阳

时间：2021年9月



课程目录

01

标准制定背景
个人信息保护原则

02

数据来源的合法基础

03

数据保留与使用
数据对外提供

04

特殊类型的和儿童的个人信息

05

供应商管理

06

数据主体的权利
数据安全保护

07

数据境外提供
数据泄露与数据安全事件响应

第五课 供应商管理

供应商遴选 及入库审查

数据供应商入库审查单

供应商名称: ←

审查部门: ←

审查日期: ←

审查结果: ←



审查要素	审查重点	审查结果
1. 基本信息	供应商的基本信息的真实性、准确性和完整性,如营业执照、行政许可或备案(如需)、银行开户、税务登记等;重点审核供应商是否为中国法律合法成立并有效存续的公司,是否能从“国家企业信用信息公示系统”查询到其企业信息	
2. 资质证明	审核供应商是否有相关资质证明,其经营范围是否满足需求	
3. 数据安全管理制度及技术措施	审核供应商内部是否有相关数据安全管理制度及数据安全保护技术措施,并审核证明材料的真实性、准确性、完整性和有效性	
4. 数据活动合规性	审核供应商收集使用个人信息是否符合《中华人民共和国网络安全法》、《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》、《信息安全技术个人信息安全规范》等法律法规和司法解释的要求。具体包括是否制定并公开数据收集使用规则,是否违反收集使用规则使用个人信息的情况,是否明示收集使用个人信息的目的、方式和范围,是否经个人信息主体同意收集使用个人信息,是否发生过数据泄露等方面	

» 第五课 供应商管理

供应商遴选及入库审查

- 供应商的基本信息的真实性、准确性和完整性，如营业执照、行政许可或备案(如需)、银行开户、税务登记等；重点审查供应商是否为中国法律合法成立并有效存续的公司；
- 供应商是否有相关资质证明，其经营范围是否满足合作需求；
- 供应商内部是否有相关数据安全管理制度及数据安全保护技术措施；
- 供应商收集使用个人信息是否符合《中华人民共和国网络安全法》、《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》、《信息安全技术个人信息安全规范》等法律法规和司法解释的要求。具体包括是否制定并公开数据收集使用规则，是否违反收集使用规则使用个人信息的情况，是否明示收集使用个人信息的目的、方式和范围，是否经个人同意收集使用个人信息，是否发生过数据泄露等方面；
- 供应商是否有行政处罚的信息，是否曾被列入经营异常名录；
- 供应商作为被告的涉诉情况，是否被列入严重违法失信企业名单；
- 供应商以往项目完成质量，配合度等。

第五课 供应商管理

供应商承诺函

研究服务提供者在与供应商合作时，应要求供应商说明个人信息来源，并以合同或者承诺函形式对其个人信息来源的合法性进行确认。

供应商数据安全承诺函

公司名称:

地 址:

致 XXXX 公司:

感谢贵司信任，接受_____公司（以下简称“我司”）申请，将我司纳入贵司潜在的供应商名录，给予未来可能存在的合作机会。为建立稳定健康、可持续发展的合作关系，维护双方的共同利益，现特就我司在数据安全方面向贵司作出如下承诺：

1. 我司承诺，我司为中国法律合法成立并有效存续的公司，我司企业运营符合法律法规要求。
2. 我司已建立严格信息及数据安全使用管理制度及内部安全管理制度和操作流程，控制信息及数据知悉范围，并与知悉信息及数据的工作人员签订保密协议，确保知悉信息及数据的工作人员遵守保密义务。
3. 我司承诺，在合作过程中的个人数据收集、数据处理、数据存储等均符合所在国或活动所处法域的个人数据保护相关的法律要求。这些要求包括但不限于：
 - 1) 收集的信息必须是依据我司法定义务，或我司履行协议之必要行为；
 - 2) 收集信息时必须明示被收集的公司或个人，并得到被收集方的明示同意；
 - 3) 信息的收集必须在必要限度范围内，不得收集与履行协议无关或不必要

» 第五课 供应商管理

供应商收集数据的合法性基础

研究服务提供者在与供应商合作时，应了解供应商收集数据是否满足合法性基础，是否已向个人充分告知并获得授权同意。

授权同意范围

研究服务提供者在与供应商合作时，应了解供应商已获得的个人信息处理的授权同意范围，包括使用目的，个人是否授权同意对外提供、公开披露、删除等。如市场研究所需进行的个人信息处理超出已获得的授权同意范围的，应在获取个人信息后的合理期限内或处理个人信息前，征得受访者或者其他个人的明示同意，或通过供应商征得受访者或其他个人的明示同意。

» 第五课 供应商管理

供应商处理数据时

8.1.1 委托者要求

研究服务提供者在市场研究中委托第三方处理个人信息时，应符合以下要求：

- 研究服务提供者作出委托行为，不应超出已征得个人授权同意的范围或应遵守5.2.4所列情形；
- 研究服务提供者应对委托行为进行个人信息安全影响评估，确认受委托者的数据安全能力；
- 研究服务提供者应对受委托者的个人信息处理进行监督；
- 研究服务提供者应准确记录和存储委托处理个人信息的情况；
- 研究服务提供者得知或者发现受委托者未按照委托要求处理个人信息，或未能有效履行个人信息隐私保护责任的，应立即要求受托者停止相关行为，且采取或要求受委托者采取有效补救措施（如更改口令、回收权限、断开网络连接、现场销毁等）处理或消除个人信息面临的安全风险。必要时研究服务提供者应终止与受委托者的业务关系，并要求受委托者及时删除从研究服务提供者获得的个人信息。

» 第五课 供应商管理

供应商处理数据时

8.1.2 受委托者要求

受委托者应符合以下要求：

- 严格按照研究服务提供者的要求处理个人信息。受委托者因特殊原因未按照研究服务提供者的要求处理个人信息的，应及时向研究服务提供者反馈；
- 未经研究服务提供者同意，受托方不得转委托他人处理个人信息；
- 协助研究服务提供者保障受访者或其他个人的权利；
- 受委托者在处理个人信息过程中无法提供足够的安全保护水平或发生了安全事件的，应及时向研究服务提供者反馈；
- 在委托关系解除时将个人信息返还个人信息处理者或者予以删除。

