个人信息安全保护

专 业 课 小 课 堂

主讲：李晶华

时间：2021年9月

课程目录

第三课 数据保留与使用以及数据对外提供

个人信息的保留

6.1 个人信息的分类存储

- 研究服务提供者应将市场研究中收集的个人信息进行妥善分类，不同来源、不同类型的个人信息应分别存储，避免数据混淆。
- 对所存储的分类个人信息应采取安全管理措施，建立使用权的分级制度，形成使用登记记录，并定期进行安全审核。

6.2 个人信息存储时间最小化

- 个人信息存储期限应为实现个人授权使用的目的所必需的最短时间，法律法规另有规定或者个人另行授权同意的除外。
- 超出上述个人信息存储期限后，应对个人信息进行删除或匿名化处理。

6.3 去标识化处理

- 收集受访者或其他个人的个人信息后，宜立即进行去标识化处理，并采取技术和管理方面的措施，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。

第三课 数据保留与使用以及数据对外提供

个人信息的使用

7.1 个人信息的访问

7.1.1 专人负责

不同来源，不同类型的个人信息应指派专人负责对其管理并形成管理日志，记录管理人员、授权人员及权限、个人信息的访问情况、下载情况等。

应当只将对于个人信息的访问权限授权给受其管理并对其负有保密义务的人员。

7.1.2 最小授权

研究服务提供者对被授权访问个人信息的人员，应建立最小授权的访问处理策略，使其只能访问职责所需的最小必要的个人信息，且仅具备完成职责所需的最少的数据操作权限。

第三课 数据保留与使用以及数据对外提供

个人信息的使用

7.1 个人信息的访问

7.1.3 内部审批

研究服务提供者在市场研究中对于个人信息处理活动应实行内部审批制度。

- 对个人信息的重要操作设置内部审批流程（如，批量修改、拷贝、下载）
- 对安全管理人员、数据操作人员、审核人员的角色进行分离设置
- 因工作原因需超权限处理个人信息的，应经个人信息保护责任人或工作机构进行审批，并记录在册
- 对个人敏感信息的访问、修改等操作，需要对角色权限处理的基础上，按照业务流程的需求触发操作授权（如，当收到受访者投诉，投诉处理人员才可以访问该个人的相关信息）

7.1.4 人员离职

人员离职时，研究服务提供者应检查其全部个人信息处理活动，及时删除其访问权限，要求其删除已下载的个人信息数据，并以合同或其他形式确认其保密义务。

7.2 个人信息的使用限制

7.2.1 已结项项目的个人信息使用

已结项或已关闭的市场研究项目中的个人信息原则上不可查询或调取，如特殊情况需要查询和调取的，应设置内部审批流程并记录在册。

7.2.2 使用范围

使用个人信息时，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围。因市场研究需要，确需超出上述范围使用个人信息的，应再次征得个人明示同意；

7.2.3 新个人信息使用

如所收集的个人信息经过加工处理而产生的新个人信息，能够单独或与其他个人信息或信息结合能识别特定自然人身份或者反映特定自然人活动情况的，应将其认定为个人信息。对其处理应遵循收集个人信息时获得的授权同意范围。

7.2.4 界面展示个人信息

涉及通过界面展示个人信息的（如屏幕显示、纸面），研究服务提供者应对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险，被访者及个人同意展示的除外。

第三课 数据保留与使用以及数据对外提供

7.3用户画像的使用限制

7.3.1 特征描述的合法性要求

用户画像中对受访者或者其他个人的特征描述，不应：

- 包含淫秽、色情、赌博、迷信、恐怖、暴力的内容；
- 表达对民族、种族、宗教、残疾、疾病歧视的内容。

个人信息的使用

7.3.2 用户画像使用要求

在市场研究或其他对外合作中使用用户画像的，不应：

- 侵害公民、法人和其他组织的合法权益；
- 危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、 民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序。
- 除为实现受访者或个人授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。

第三课 数据保留与使用以及数据对外提供

个人信息的使用

7.4使用目的变更时的告知同意

研究服务提供者因市场研究需要需变更使用目的的，需向个人告知涉及的个人信息类型、变更原因、变更后的处理目的，并再次征得个人的明示同意。使用目的变更包括但不限于以下情形：

- 研究服务提供者收集受访者或其他主体个人信息后，超出原有授权范围使用的；
- 研究服务提供者间接获取个人信息后，进行加工处理形成新的个人信息并用于其他目的；
- 研究服务提供者进行收购、兼并等，将获取的个人信息超出原有授权范围使用的；
- 研究服务提供者收集后涉及重大处理规则变化的，例如需要将个人信息传输到境外进行处理的。

第三课 数据保留与使用以及数据对外提供

个人信息的对外提供

- 个人信息的委托处理
- 个人信息的第三方提供
- 收购、兼并、重组、破产时的个人信息转让
- 个人信息公开披露
- 对外提供个人信息不必征得个人的授权同意的情形

第三课 数据保留与使用以及数据对外提供

委托者要求（委托第三方处理个人信息）

- 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（征得授权同意的例外，如法律法规、国家安全、公共安全、个人生命财产安全等）所列情形；
- 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；
- 应对受委托者的个人信息处理进行监督；
- 应准确记录和存储委托处理个人信息的情况；
- 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。

第三课 数据保留与使用以及数据对外提供

受委托者要求

- 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。

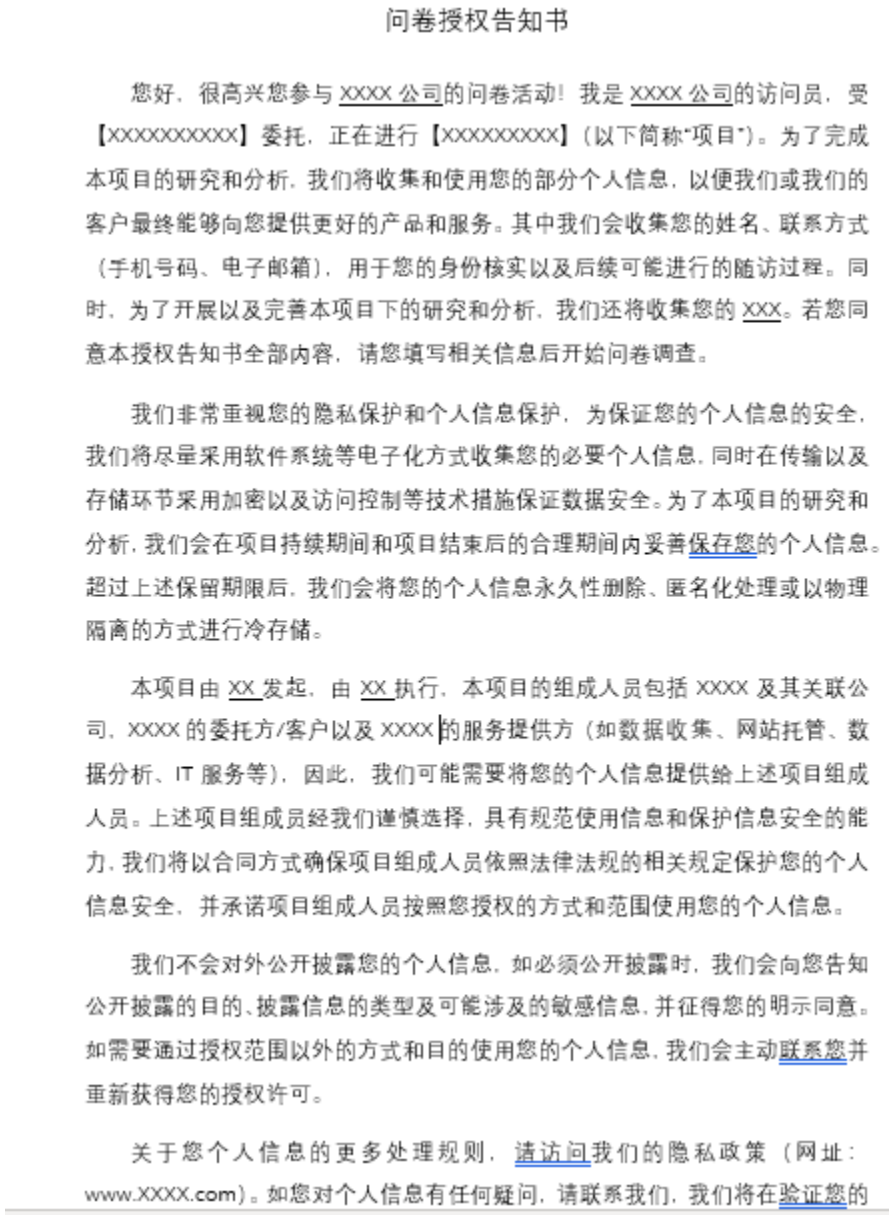
第三课 数据保留与使用以及数据对外提供

授权同意

个人信息第三方提供

研究服务提供者在市场研究中应仅向客户及其他第三方提供匿名化处理后的受访者或其他个人的个人信息，或仅提供统计分析结果，除非：

- 已向受访者或其他个人告知第三方的身份、个人信息的处理目的、处理方式和个人信息的种类，并事先征得受访者或其他个人的授权同意；
- 提供经去标识化处理的个人信息，且确保个人信息接收方无法重新识别或者关联个人。



问卷授权告知书

您好，很高兴您参与 XXXX 公司的问卷活动！我是 XXXX 公司的访问员，受【XXXXXXXXXX】委托，正在进行【XXXXXXXXX】（以下简称"项目"）。为了完成本项目的研究和分析，我们将收集和使用您的部分个人信息，以便我们或我们的客户最终能够向您提供更好的产品和服务。其中我们会收集您的姓名、联系方式（手机号码、电子邮箱），用于您的身份核实以及后续可能进行的随访过程。同时，为了开展以及完善本项目下的研究和分析，我们还将收集您的 XXX。若您同意本授权告知书全部内容，请您填写相关信息后开始问卷调查。

我们非常重视您的隐私保护和个人信息保护，为保证您的个人信息的安全，我们将尽量采用软件系统等电子化方式收集您的必要个人信息，同时在传输以及存储环节采用加密以及访问控制等技术措施保证数据安全。为了本项目的研究和分析，我们会在项目持续期间和项目结束后的合理期间内妥善保存您的个人信息。超过上述保留期限后，我们会将您的个人信息永久性删除、匿名化处理或以物理隔离的方式进行冷存储。

本项目由 XX 发起，由 XX 执行，本项目的组成人员包括 XXXX 及其关联公司，XXXX 的委托方/客户以及 XXXX 的服务提供方（如数据收集、网站托管、数据分析、IT 服务等），因此，我们可能需要将您的个人信息提供给上述项目组成人员。上述项目组成员经我们谨慎选择，具有规范使用信息和保护信息安全的能力，我们将以合同方式确保项目组成人员依照法律法规的相关规定保护您的个人信息安全，并承诺项目组成人员按照您授权的方式和范围使用您的个人信息。

我们不会对外公开披露您的个人信息，如必须公开披露时，我们会向您告知公开披露的目的、披露信息的类型及可能涉及的敏感信息，并征得您的明示同意。如需要通过授权范围以外的方式和目的使用您的个人信息，我们会主动联系您并重新获得您的授权许可。

关于您个人信息的更多处理规则，请访问我们的隐私政策（网址：www.XXXX.com）。如您对个人信息有任何疑问，请联系我们，我们将在验证您的

第三课 数据保留与使用以及数据对外提供

个人信息的第三方提供

8.2.2 个人信息提供者要求

研究服务提供者在市场研究中对外提供个人信息时，应充分重视风险。对外提供个人信息，非因收购、兼并、重组、破产原因的，应符合以下要求：

- 事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人的措施；
- 通过合同等方式规定双方的责任和义务；
- 准确记录和存储个人信息的对外提供情况，包括对外提供的日期、规模、目的，以及个人信息接收方基本情况等；
- 研究服务提供者发现个人信息接收方违反法律法规要求或双方约定处理个人信息的，应立即要求个人信息接收方停止相关行为，且采取或要求个人信息接收方采取有效补救措施（如更改口令、回收权限、断开网络连接等）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解除与个人信息接收方的业务关系，并要求个人信息接收方及时删除从研究服务提供者获得的个人信息；
- 因对外提供个人信息发生安全事件而对个人合法权益造成损害的，研究服务提供者应承担相应的责任；
- 帮助个人了解个人信息接收方对个人信息的存储、使用等情况，以及个人的权利。

第三课 数据保留与使用以及数据对外提供

个人信息的第三方提供

8.2.3 个人信息接收者要求

客户及其他第三方在市场研究中作为接收方，接收个人信息时应符合以下要求：

- 履行合同约定的责任和义务；
- 在个人的授权同意范围内处理个人信息；
- 超出个人的授权同意范围处理个人信息的，应重新向个人告知并取得其同意；
- 接收匿名化或去标识化后个人信息的，接收者不得利用技术手段重新识别个人身份。

第三课 数据保留与使用以及数据对外提供

个人信息的第三方提供

8.3 收购、兼并、重组、破产时的个人信息转让

当研究服务提供者发生收购、兼并、重组、破产等变更时，对研究服务提供者的要求包括：

- 向个人告知有关情况；
- 变更后的个人信息处理者应继续履行原个人信息处理者的责任和义务，如变更个人信息使用目的时，应重新取得个人的明示同意；
- 如破产且无承接方的，对个人信息作删除或销毁处理。

第三课 数据保留与使用以及数据对外提供

个人信息的第三方提供

8.4 个人信息公开披露

个人信息原则上不应公开披露，研究服务提供者经法律授权或具备合理事由确需公开披露时，应符合以下要求：

- 事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人的措施；
- 向个人告知公开披露个人信息的目的、类型，并事先征得个人明示同意；
- 准确记录和存储个人信息的公开披露的情况，包括公开披露的日期、规模、目的、公开媒体/平台、公开范围等；
- 承担因公开披露个人信息对个人合法权益造成损害的相应责任。

谢 谢！

主讲：李晶华

时间：2021年9月