



全球调研准则和指导原则

ESOMAR资料保护备忘录

ESOMAR是资料分析、调研和社区洞察力的全球代言人，代表4900多名个人专业人员和500多家公司在130多个国家提供或委托进行数据分析和调研，这些国家全部同意维护ICC/ESOMAR国际准则。

© 2017 ESOMAR。2017年9月发布。

本指南以英文撰写，英文版本（www.esomar.org）为最终版本。在适当归属并且包含以下通知“© 2017 ESOMAR”的情况下，可以复制、分发和传输文本。

目录

1	引言	4
2	范围	4
3	“必须”和“应该”的用法	5
4	定义	5
5	资料保护政策和程序的自助备忘录	6
5.1	影响最小	6
5.2	通知和同意	6
5.3	诚信/安全	8
5.4	资料传输	9
5.5	跨境个人资料转移	10
5.6	外包和分包	11
5.7	隐私声明	11
6	特别问题	11
6.1	收集来自儿童、年轻人和其他弱势群体的资料	12
6.2	企业对企业调研	12
6.3	照片、音频和录像	12
6.4	云储存	12
6.5	匿名和假名	13
7	来源和参考	13
8	项目团队	13

1 引言

在全球范围内工作的调研人员越来越多地面临着旨在确保尊重个人隐私和保护个人资料的一系列国家法律。在全球化这一大背景下工作的调研人员越来越多地要面对各国为确保尊重个人隐私和保护个人资料而制定的一系列法律。

与此同时，新技术难以阻挡地扩展到我们生活的方方面面，这不仅增加了调研人员可能获取到的个人资料量，更引入了必须给与保护的新类型的个人资料。

有一点没有改变，就是调研人员需要通过维护资料主体权利的实践来维护市场、民意调查、社会研究和数据分析的声誉，并保持对调研成果的信心。

2 范围

本文档的目的在于向调研人员（尤其是在资料保护要求方面可能不具备广泛资源或经验的小型机构任职的人士）提供关于其在全球资料保护框架内职责的总体指导准则，从而确保资料主体保持其对个人资料的掌控。所使用的具体框架是由经济合作与发展组织（OECD）制定的。该框架包括一套用于设计程序以确保隐私和保护个人资料的八项原则：

- 收集限制
- 资料质量
- 目的规范
- 使用限制
- 安全保障
- 开放性
- 个人参与
- 问责制

这些广泛的原则在全球大部分现有和新制定的隐私及资料保护法律中得以体现。

不过，调研人员应注意到，OECD与欧盟的资料保护要求关系最为紧密，因而在其他区域工作的调研人员被要求查阅可能适用的其他框架。这些框架包括：《亚太经合组织隐私框架》、《欧盟-美国隐私保护框架》、《瑞士-美国隐私保护框架》、美国注册会计师学会(AICPA)和加拿大特许会计师学会(CICA)制定的《广泛接受的隐私原则》。尽管这些框架总体上不具有法律效力，却仍表述了调研人员在相应区域工作时必须采纳的原则。

此外，调研人员在计划进行现场工作或处理资料时，必须审视并遵循每个国家的资料保护和市场调研自律要求，这是因为上述基本原则在特定国家的实施可能会有差异。本文档中的指导准则仅为最低标准，对于特定的调研项目，可能需要附加措施作为补充。调研人员可能发现有必要咨询位于将要进行调研的国家所在辖区的法律顾问，以便确保完全合规。查阅[The Data Protection Laws of the World](#)（全球资料保护法律）可能对他们有所帮助，这是由DLA Piper提供的在线资源，每年都会更新。

最后，针对特定领域（例如：医疗保健）进行调研工作的调研人员可能希望查询特定的指导准则以获取更多指导，例如[EphMRA Adverse Event Reporting Guidelines 2014](#)（《EphMRA 负面事件报导指导准则 2014》）。

3 “必须”和“应该”的用法

在整个文件中，“必须”一词用于确定强制性要求。在描述调研人员必须遵循的原则或实践时，我们使用“必须”一词。“应当”一词用于表述实施。此用意在于认可调研人员可根据其调研的设计方案而选择以不同的方法实施某项原则或做法。

4 定义

企业对企业调研(B2B)是指从企业、学校、非营利组织等法人实体收集资料。

企业对消费者调研(B2C)是指从个人或家庭收集资料。

同意是指由个人自由地给予和明确表示同意收集和处理他/她的个人资料。

资料分析是指检查资料集以发现隐藏的模式、未知的相关性、趋势、偏好和其他用于调研目的的有用信息。

资料控制者是指负责确定如何处理个人资料的个人或组织。例如，调研客户将是有关其客户或主顾的资料控制者；政府福利机构是其福利受益人资料的资料控制者。

资料员是指代表资料控制者并按其指示对个人资料进行获取、记录、留存或操作（包括分析）的一方。正如上文指出的那样，调研公司将同时是某项综合性调研的数据控制者和处理者。

资料主体是指其个人资料被用于调研的任何个人。

伤害是指有形伤害或物质损害（如身体伤害或财产损失）、无形或精神伤害（如声誉或商誉损害）或过度侵入私人生活，包括未经请求的针对个人的营销信息。

隐私保护法律是指与本文件中的原则相一致的国家法律或法规，这些法律或法规的执行具有保护个人资料的效果。

非调研活动是指出于改变他人态度、观点或行动之意图，而对被收集或被分析的个人资料直接采取行动的。

被动资料收集是指通过观察、衡量或记录个人的行为或行为来收集个人资料。

个人资料（有时称为个人身份资料或PII）是指任何与自然人有关、可用于识别个人身份的资料，例如对直接标识信息的提及（如姓名、特定地理位置、电话号码、照片、声音或录像），或对个人的身体、生理、心理、经济、文化或社会特征的间接提及。

主要资料是指调研人员为调研目的从个人那里收集的资料或收集的关于个人的资料。

隐私声明（有时称为隐私政策）是指一家组织的隐私做法的已发布摘要，其中描述了该组织收集、使用、披露和管理资料主体的个人资料的方式。

个人资料处理包括但不限于收集、记录、组织、存储、改编或修改、检索、查询、使用、通过传输、传播来披露或提供、整合或合并、阻止、擦除或销毁，不论是以自动的或是其他方式。

调研包括所有形式的市场、舆论和社会研究以及数据分析，是对有关个人和组织信息的系统性收集和解释。它利用应用社会学、行为学和数据科学的统计和分析方法和技术，为商品和服务提供者、政府、非营利组织和公众提供洞见并支持其作出决策。

调研人员是指从事或担任调研顾问的任何个人或组织，包括在客户组织和所使用的任何分包商中工作的个人或组织。

调研客户或资料使用者是指请求、委托、资助或订阅调研项目的全部或任何部分的任何个人或组织。

二手资料是指为了其他目的和之后用于调研而收集的资料。

敏感资料是指当地法律要求尽可能按最高标准给予保护使之免受未经授权访问的特定类型的个人信息，以便保护个人或组织的安全或隐私，此类信息的处理需得到资料主体额外的明确许可。敏感资料的界定因管辖范围而异，可包括资料主体的种族或族裔出身、健康记录、性取向或性习惯、犯罪记录、政治观点、贸易协会成员资格、宗教或哲学信仰、位置、财务信息和诸如服用管制药品或酒精等违法行为。

资料的**传输**是指资料的任何披露、通讯、拷贝或从一方到另一方的移动（不论采用何种介质），包括但不限于跨网络移动、物理意义上的传输、从一个介质或设备到另一介质或设备的传输，或远程访问资料。

个人资料跨境转移是指以任何方式跨境移动个人资料，包括从资料收集国以外的国家访问资料以及针对资料使用云技术。

弱势群体是指作出自主知情决策能力有限的个人，包括那些有认知障碍或交际障碍的个人。

5 资料保护政策和程序的自助备忘录

以下备忘录的使用者可能意识到标题和项目次序与OECD所采用的有所不同。此处的意图在于采用调研人员更为熟悉的语言和次序来表述原则。读者也可能认识到各个条目互相关联，有时出现重叠。然而，将此备忘录视作一个整体这很重要，各个条目应看作是相互补充而非排斥的，特别注意那些取决于组织是作为资料控制者还是处理者的差异。任何答案不是“是”的问题意味着隐私保护计划的潜在差距，因而存在违反一项或多项资料保护法律的潜在风险。

5.1 影响最小

1. 在设计调研项目时，您是否将个人资料的收集限定为仅对调研目的有必要的那些项目，并确保不会以与这些目的不相符的方式使用资料？

调研人员必须只收集、获取和/或持有从质量控制、抽样和/或分析角度来看确有必要的个人资料。如果是B2B调研，这包括关于资料主体在组织中的职位或级别的个人资料，因为这对达成调研目的确有必要。

同样的原则适用于被动资料收集方法以及在处理二级资料来源时。因而，调研人员有责任确保只有调研中使用的资料对于调研目的确有必要。如收到其他个人资料，必须将其过滤并删除。

2. 您是否实施了相关流程，以确保资料主体不因其个人资料用于市场调研项目而导致遭受损害或负面影响？

调研人员必须确保个人资料无法被跟踪，且无法通过调研结果借助交叉分析（推论披露）、小型取样或其他任何方法推断个人资料主体的身份。例如，合并诸如地理区位资料等辅助信息，或能够在客户满意度调研中识别出特定的雇员。

3. 如您打算聘用分包商或其他第三方供应商代表您履行服务，您是否披露履行双方同意的服务所必须的最少量的个人资料？您是否订立了合同可确保对方也提供类似的保护级别？

在聘用分包商期间，仅向其提供履行双方同意的服务所必须的最少量的个人资料，通过合同和说明使分包商时刻明确其在拥有这些资料期间应承担的责任。所有分包商必须遵循与调研机构同样的规则和法规。此外，只在事先获得同意或得到调研机构的客户授权后，方可向分包商或其他第三方供应商传输个人资料。

以上规定假定调研中使用的所有资料将保持机密，且仅会在合并层面上进行分析和报告。如资料主体同意将其回答与其个人资料关联，则必须向其告知信息将如何共享和使用。

5.2 通知和同意

4. 在进行主要资料收集时，您是否征得个人资料将被收集的每一位资料主体的同意？

根据OECD隐私原则，任何个人资料均应当以合法正当的途径获取，并且如果适用，应得到资料主体的知情或同意。总体而言，各国法律提供了诸多合法公平的基础，但在大多数情况下，调研人员将被要求征得资料主体的同意。

同意必须是：

- 自由的（自愿且能够随时取消）；
- 具体的（与一个或多个可识别的目的相关）；且
- 知情的（完全知道给予同意的所有相关后果）。

在已向资料主体提供下文中规定的信息后，还必须通过声明或行动明确地表示同意。简而言之，应向资料主体告知（1）其个人资料将用于何种目的；（2）具体要收集哪些资料；（3）收集资料的企业或机构的名称、地址和联系信息，如不是同一家单位，则应告知资料控制者的相关信息；（4）是否会将信息披露给第三方。

调研人员应慎重考虑采用何种方式征得同意，通常表述为自愿退出、自愿参与、暗指或明示。所选择的具体方法应记录在案。

总体而言，资料收集越是敏感、侵入性越强或不够明显，所需的同意的标准越高。在某些辖区，定义了资料收集前需征得有关个人明确同意的“敏感个人资料”的级别。

调研人员有可能无意中或从尚未被定义为资料主体的人员处收集到或接收到个人资料。例如主动提供的信息；客户提供的含有超出开展调研所需的更多信息；以及从照片或视频上捕获的无关人员。调研人员在处理此类信息时应采用与针对其他个人资料时的同样方式。应立即使此类资料无法识别或将其销毁，尤其是在无法向资料被收集人告知资料下落、存储或用途时。在某些法律辖区，强制要求删除此类资料或采用针对有意获取的其他信息完全相同的方式处置此类信息。

5. 您是否清楚收集和维持资料的目的？

调研行业长久以来一直将调研与为了其他目的而收集资料（例如广告、促销、名单开发、直接营销、直销）区分开来。这一差别对于区分目的和在监管机构及公众中创造良好印象非常重要。近年来，新技术的出现为通过在线追踪和可下载移动应用等技术来收集个人资料提供了便利。任何情况下，在收集任何资料前，都必须告知潜在的资料主体其资料将用于何种目的、可能产生何种潜在后果，包括出于质量目的而跟进联系。

当调研人员出于市场调研目的而从资料主体收集个人资料，务必注意要对资料主体保持信息透明。关于收集的个人资料将用于何种目的以及与第三方的任何分享等信息必须充分传达给资料主体。例如，如果计划将个人资料用于把调研答复与客户简介相关联，在收集资料时就应告知资料主体。

必须定期审核隐私政策，以确保所收集的资料类型和计划中的用途未发生改变。调研人员必须确保在调研机构中实际所采用的业务做法和技术与向资料主体做出的承诺相一致，并符合不断演化的监管要求。必须对每一项提议的个人资料用途进行分析，以确保遵从地方隐私法律、ICC/ESOMAR关于市场、舆论、社会研究和数据分析的准则以及ESOMAR/GRBN指导准则，并与向资料主体做出的隐私承诺相一致。

6. 您是否清楚具体要收集哪些资料？

鉴于在特定管辖权对个人资料的宽泛定义，在制定隐私政策时应考虑到可能要收集的所有可能的个人资料要素。个人资料可能包括姓名、地址、电邮地址、电话号码、手机号码、出生日期、移动设备标识符、IP地址、照片、音视频记录、身份证号（驾照、社保、国家保险）、机构指派的用户识别号、社交媒体用户名、cookie或追踪像素/标签中存储的资料。还应谨记：单个资料项本身可能不被地方法律视作可识别身份的资料，但与其他资料结合（例如邮编、性别、工作地点或学校、职务、薪金），则可能致使个人身份被披露。

此外，应考虑到个人资料所有可能的接收者。调研人员、调研机构、第三方服务提供者和/或最终客户在调研项目过程中都可能有能力收集和/或使用个人资料。

7. 您是否明确说明资料将如何收集，包括资料主体可能不知情的任何被动资料收集？

以往，调研主要依赖面谈作为首要的个人资料收集方法。如上文第5点所述，新技术使在个人不知情的情况下收集更广泛的个人资料成为可能。必须将搜集的具体资料及用到的收集方法告知各个资料主体，不论是通过主动方式（例如访谈）或是被动方式（例如移动应用或通过在线cookie追踪）。

调研人员应考虑到所收集的资料中的哪些要素和/或资料收集方法可能是资料主体意想不到的，并针对这些收集方法重点给予说明。请考虑在更详尽的隐私政策上部放置“简易形式”的隐私政策，用以描述可能意想不到的或是唐突的资料收集或使用行为。移动应用，尤其是涉及到地理位置、“被动监听”和/或移动设备操作系统测量的那些应用，都需要详细说明，并从这些活动的资料主体那里征得明确的同意。

8. 在将所收集的个人资料用于调研以外的某些目的（例如客户资料、社交媒体资料等），您是否确保用途合法并且确保资料主体的权益得到保护？

调研人员及类似的非调研人员越来越多地寻求获取和使用二级资料，用以补充或替代主要资料收集。在访问和处理此类资料前，调研人员必须确保其既定用途资料收集的初始目的相一致。他们必须验证原始收集是合法的，得到了资料主体明确或暗示的同意。此外，他们必须通过确保仅用于调研目的来维护正当利益。

调研人员还必须规划其调研工作，确保后续资料处理不对资料主体产生损害风险。调研人员必须将防护措施落实到位，以规避此类损害的风险，例如未经事先同意，个人资料主体的身份不会泄露或披露，采取措施降低资料粒度，降低个人身份被辨识的几率，确保不会由于其资料用于调研目的而导致对资料主体进行任何非调研活动。

5.3 诚信/安全

9. 是否为了确保所有个人资料的准确、完整和最新而制定了流程？

在调研过程的每一个阶段都应进行质量检查。在制定调研问卷或调研应用时，在开始现场工作之前应进行测试，以便将资料收集出错的风险降到最低。在现场工作阶段，应按照适用的调研质量标准开展访谈的监控和验证。在资料处理和报告阶段，应进行额外的质量检查，从而确保资料正确，且分析、结论、建议与资料一致。

调研运作小组应确保小组成员能够随时审核和更新其概况资料，应定期提醒他们这样做。从小组提取的样本应标注最新的人员信息。这方面的一个很好的标准做法来源是ISO 26362:2009 – 市场、舆论、社会研究中的访问小组。

使用二级资料时，调研人员应审核资料收集时部署的质量检查举措，确保资料准确。

10. 您是否确保个人资料留存时间不超过信息收集、获取或后续处理所需的时间？您是否制定了流程，在不再需要资料时可以单独存储标识符或从资料记录中删除标识符？

调研人员应将资料留存时间设置得尽量短暂，但在任何情况下都应遵照适用的法律、所收集的个人资料的来源、其是作为数据控制者还是处理者来工作。如果是后者，客户可通过合同强制规定存留时间。

关于个人资料的来源，来自于纵向调研的信息或关于成员的简介信息通常在其作为活跃成员的整个阶段期间使用和留存。相反，参与对于临时性调研的非成员资料主体的个人资料，应采用更短的留存时间。显然，请勿过快地销毁其个人资料，因为要在资料处理阶段进行质检，以确保准确性并满足资料完整性隐私原则的要求。

当使用个人资料时，调研人员最好应使用匿名标识符。对于将资料主体的名称、地址、电话号码与相应的内部ID号相关联的主文件，必须安全保管，仅限有限几个人获取，例如抽样或小组管理人员。如此一来，因工作需要而要分析个人层级资料的调研人员、资料处理或编码人员可在不看到资料主体的姓名、地址或电话号码的情况下进行数据分析。

当调研回复已处理并以合并方式报告，应删除统计资料、资料主体的个人资料以及相应的匿名标识符，使得调研机构不再持有个人资料。

11. 是否制定了程序，用以回应资料主体关于从其获取的个人资料的请求？您的处理来自资料主体访问请求的程序是否包含鉴定资料主体身份、在合理时间内回应请求、允许其纠正不准确信息或彻底删除资料？

应制定、沟通并遵循正规的程序，以便回应个人资料被机构所持有的资料主体想要访问个人资料的请求。应对提出访问请求的资料主体的身份进行鉴定，这对于预防以不当方式将个人资料披露给他人至关重要。

一旦提出访问请求的资料主体的身份得以鉴定（此人为自称是资料主体的人，有权访问所述个人资料），调研人员应尽快全力满足其访问请求，例如：在10到30天内，具体时间取决于适用的法律。如调研机构需要额外时间满足其要求，则可延长法律中规定的期限，前提是通知此人并且延期的理由合理。更多的时间可能是有必要的，例如：进行查询或从多个数据库和数据源收集所要的信息。

不过，资料保护法律可能含有要求机构在特定情况下拒绝资料主体个人信息访问权的免责条款，但这些免责条款对于用于调研目的而正在收集的资料很可能并不适用。例如，如果信息属于律师-客户豁免权，适用的法律可能允许机构拒绝访问请求。另一个例子，如果机构因执法或国家安全原因而将信息披露给政府机构，该政府机构可能要求调研机构拒绝个人访问信息或不得透露信息已被披露之事。

12. 是否针对每个资料集制定了安全协议，以防止遗失、未经授权访问、销毁、修改或披露？

履行这些职责首先要制定并实施安全政策，以保护个人信息和其他类型的机密信息。可依据ISO 27001这一广为认可的信息安全标准制定完整的安全政策。

采用适当的安全举措以提供必要的安全保护，这些举措包括：

- 物理性措施（文件柜上锁、限制进入办公室、报警系统、安全摄像头）
- 技术性工具（密码、加密、防火墙）
- 组织性控制（背景核查、关于携带电脑离开的规定、基于“需要知道”来限制访问、人员培训、与客户和分包商订立协议）

安全政策还应包括处理导致个人资料泄露的潜在资料违规的程序。如果是其他方收集的二级资料，例如客户数据库，则必须立即通知该方。如果资料披露会给资料主体带来某些风险（例如身份被窃），则必须通知资料主体，并采取适当步骤防止风险发生。

13. 是否有关于个人资料留存时间的明确声明？

个人资料留存时间的长度可能因调研项目而异，取决于多种情形，在对问题9的回答中曾提及。

尽管隐私政策中应含有通常的留存做法，但对于不同种类的调研，并不一定总是能够精确地说明留存时间。因而，调研人员还应考虑到在招募材料、问卷说明或特定调研的同意书中阐明资料留存时间。他们应准备好按要求针对给定项目阐明资料留存时间期限。

5.4 资料传输

14. 您是否有明确的规则和流程以管制个人资料的使用和披露？

这些规则和流程在存在于您的国家的当地隐私和资料保护法律中有明确规定。对其含义的解释应和

流程及书面文档一起清晰记录，以确保人员能够实施这些关于个人资料管理的流程，并熟知这些规则和流程。例如，这将包含这样的原则：这些资料在得以披露前需要征得资料主体的同意，即便是透露给客户或客户机构内部的调研人员，不论资料是否是由调研人员还是其他各方收集的。

15. 是否清晰明确地阐述了在何种情况下可以披露个人资料？

资料主体必须知悉其个人资料出现了何种情况，必须以资料主体同意的口头或某些书面形式或文档做出说明，例如：通过记录在案作为已同意的证据的同意书。

16. 您的员工是否知悉这些规则并接受了实施流程培训？

您的隐私政策阐述了贵公司的资料收集和管理做法。制定内部标准作业流程对于确保兑现对资料主体的承诺也同样重要。

关于隐私的员工培训应包括适用法律概述、行业行为准则、贵公司消费者隐私政策以及SOP。应至少每年都举行隐私培训，应妥善保管参训者记录。

所有与资料主体互动的一线员工应能够高屋建瓴地阐释公司的政策和流程。他们应清楚如无法回答客户质询时应求助于哪些内部人士。

应制定清晰的监管和责任，包括针对正在执行的流程进行某些形式的监控。

5.5 跨境个人资料转移

17. 如个人资料将要从一个管辖区传输至另一管辖区，是否同时满足起源地和目的地的资料保护要求？

这常称作“跨境个人资料转移”。当跨境收集资料和/或资料处理是离岸进行的或被外包给另一国家（例如：当客户采用另一国家的调研人员开展调研，调研过程中采用客户提供的顾客或服务使用者资料）。每个国家针对此类资料如何处理和保护都制定了自己的规则，调研人员必须遵守。尽管这看起来很复杂，但如果将调研人员面临的合规问题划分为三大类就可化繁为简：

- 确保个人资料的跨境转移符合适用的国际和国家法律、法规和框架。确保跨境转移得以充分保护的最常见手段是征得资料主体同意或采用恰当的合同条款，以及如果适用的国家法律有要求，从该国资料保护机构或其他适用的隐私管制机构获得提前授权，以使用这些合同。作为额外的安全举措并且为了进一步在资料离岸处理地降低风险，应删除可识别身份的个人资料（如果适用），从而只是匿名 ID 用于将资料主体的身份关联至个人层面的资料。
- 调研人员在作为资料处理者时，例如在利用客户提供的样本开展调研时，可进行跨境转移的范围。即便调研人员以谨慎地确保跨境转移遵守传输管制规则，仍应牢记：在作为资料处理者代表资料控制者（例如调研客户）处理个人资料时，其作为资料控制者也许不能允许其掌控的个人资料被跨境转移，这可能影响到他们如何开展项目。上述双方之间应为此签订书面协议。
- 涉及到其他国家主体的个人资料（例如：以居住在不同国家的资料主体为对象的在线调研）跨境转移至调研人员正在控制此项调研之处。通常，适用的隐私法律为调研人员所在国的法律。然而，调研人员还需确保此项调研或小组遵从资料收集地所在国的其他任何适用的国家法律。推荐的做法包括确保：（1）在所有的招募材料中明确表述出调研人员的法律细节（公司名称、邮寄地址等），包括国家名称；（2）所采用的在线隐私政策包括简单明了的声明，阐明通过参与此项调研或小组而进行的跨境转移；以及（3）在小组招募同意书问题中提及跨境转移。

5.6 外包和分包

18. 是否有关于对任何外部资料处理者或其他分包商进行监督的明确要求？

当有任何形式的资料传输时，必须要有明确的要求向所有外部资料处理者或其他分包商阐明，使之遵循所需的与个人资料有关的资料保护规则。任何资料的传输都应有额外的保护，不论是个人层面或时合并的资料，要采用专用的IT流程（例如传输时对资料加密）或采用安全的FTP传输平台。如果分包商或外部资料处理者要对任何资料制作拷贝作为备份，那么必须要求清晰的流程以在存储期间保护资料，并在不再需要资料时将其删除。

19. 是否与所采用的所有分包商订立了协议（合同）？

必须与任何参与调研的分包商订立协议。合同应解决参与调研的业务条款（包括工作声明、术语、保险等）以及：

- 资料保护要求；以及
- 信息安全要求。

5.7 隐私声明

20. 关于您的隐私和个人信息保护计划的信息是否可以随时获得，并且以参与者容易理解的形式提供？

许多司法管辖区要求在资料主体容易获得的隐私声明中提供信息。尽管所要求的内容和细节因国家而异，但调研人员必须时刻向资料主体明确地表明身份，并确保阐明调研的目的，个人资料如何收集，将如何管理（收集、存储、使用、访问和披露），以及如何获取更多信息或发起投诉。

调研人员必须确保政策通俗易懂、与读者密切相关、便于定位、尽可能准确、根据机构的运作量身定制。这包括以尽可能多的语种提供隐私政策，定期审阅，酌情更新。

21. 资料控制者的身份和责任是否明晰？

调研人员必须确保其自身角色和管理个人资料的职责对于资料主体是明晰的。这包括明确资料控制者身份，以及是否使用了外部资料处理者。资料主体必须要清楚哪家机构最终会对资料的管理承担责任。

某些管辖区还要求要有专人对公司的资料保护做法负责。

如果是采用客户提供样本的不知情调研，应在访谈一开始便告知参与者在调研结束前将不会透露客户名称，因为过早透露此信息可能导致回答有偏见。由于许多国家的资料保护法律给予了资料主体法律权利，允许其知道调研人员是从何处获取的个人信息，调研人员必须做好准备随时按要求表明客户名称。

22. 是否明确说明了无论资料位于何地，资料控制者都应对其控制的个人资料负责？

如果调研人员可能要外包资料处理工作的任何部分或在管辖区之外传输资料，那么应准备好向资料控制者提供分包商的详细信息和资料处理的地点。如有必要，还应事先以书面方式从资料控制者征得同意。如果调研机构是资料控制者，他们应包括资料处理者的使用参考，如果有关，还应在其隐私政策中列出国家或宽泛的区域。调研人员应该警惕一些司法管辖区禁止调研人员将个人资料传送到没有同等资料保护法律的国家或地区。在遵守有关地方国家法律规定的跨境转移规则的情况下，大多数司法管辖区允许跨越国界组传送个人信息，尽管有些人仍然需要向资料主体通知资料可能驻留的地点。

6 特别问题

6.1 收集来自儿童、年轻人和其他弱势群体的资料

调研人员在收集任何已经为其指定法定监护人的资料主体的个人资料之前，必须征得父母或责任成人的同意。在征得同意时，调研人员必须提供有关调研项目性质的充分信息，以便父母或负责任的成年人对资料主体的参与作出明智的决定。这包括：

- 进行调研的调研人员/组织的名称和联系方式；
- 从资料主体收集的资料的性质；
- 解释资料如何被保护和使用；
- 解释要求儿童参与的原因以及可能的好处或潜在的影响；
- 说明给予和核实同意的程序；以及
- 要求父母或负责任的成人的联系地址或电话号码，以核实同意。

调研人员还应该记录责任成人的身份和他/她与资料主体的关系。

目前国际上对儿童或年轻人没有一个统一的定义。即使在一个国家内，定义也可能有所不同。基于特征（例如认知能力）而非年龄的其他定义来进行划分并在调研中采用此定义即便不是不可能也是很困难的。因此，调研人员必须依赖适用的当地法律，行为准则和文化规范中所表达的任何相关定义。在没有明确指导的情况下，ESOMAR和GRBN建议将儿童定义为12岁以下，年龄在13岁至17岁之间。如需更多详细信息，请查询ESOMAR指导准则[儿童和青少年访谈](#)。

6.2 企业对企业调研

大量的调研项目涉及收集企业，学校，非营利组织和类似组织的法律实体的资料。这种调研往往涉及及收集有关实体的信息，如收入、员工人数、部门、地点等等。

在所有这些情况下，参与组织都有权获得与报告中的身份披露相同水平的保护，例如提供给其他形式调研的个人。

值得注意的是，许多国家资料保护法律将个人的职务和单位联系信息视作个人资料。某些资料保护法律更将其要求应用到自然人和法人（例如个人和法人实体）。

6.3 照片、音频和录像

作为调研过程的一部分，许多新的调研技术创建、存储和传输照片、音频和视频记录。两个突出的例子是民族志和神秘购物。

调研人员必须认识到，对于照片，音频和录像属于个人资料，必须这样处理。如果调研人员要求资料主体以这些形式提供信息，他们还应该就如何减少非请求资料的收集，特别是从非参与者收集资料提供指导。

最后，某些类型的观察性调研可能涉及在公共场合拍摄、录像或录制涉及未被招募为资料主体的人。在这种情况下，调研人员必须获得许可，才能分享来自资料主体的这些脸部清晰可见并可识别的图像。如未获得许可，资料主体的图像应打上马赛克或给予匿名。此外，应放置清晰易见的标示，以便指明观察区，并给出责任人或机构的联系信息。摄像机的位置应该只监视观察区域。

6.4 云储存

应该仔细考虑将个人资料存储在云中的决定。调研人员必须评估云存储服务提供商的安全控制及其标准条款和条件。许多云存储服务提供商在发生安全漏洞和个人资料泄露的情况下提供较低的赔偿。这意味着调研人员的公司将面临相当严重的隐私泄密导致的财务损失和损失风险，从而对受影响的资料主体造成损害。

因此调研人员应该实施补偿性的控制措施来防范这种风险。例如，他们应该在移动（从云转移到云

中)和静止(存储在云提供商的服务器上)时加密个人资料。调研人员还应该考虑购买网络责任保险。

调研人员还必须考虑存储个人资料的物理位置,以确定云存储的使用是否是跨境转移。请参阅本文档的第5.5节进一步讨论。一些云服务提供商在某些情况下提供适合特定国家的存储位置。

最后,调研人员应该将个人资料放在私有云上,而不是公共云上。私有云是将特定数据中心的专用设备分配给调研人员的公司。私有云的主要好处是调研人员总是知道个人资料的位置。相比之下,公共云可能会导致资料位于两个或更多数据中心和两个或更多的大陆,从而提高了可能的合规性问题,既有资料保护法的适用要求,也有与资料控制者签订的合同指定个人资料必须位于何处。

6.5 匿名和假名

调研人员的资料保护责任的一个关键部分是在发布之前将资料解除识别给客户甚至公众。匿名化是一种保护措施,涉及删除或修改个人标识符以将资料转换为不能识别个人身份的形式。例子包括模糊的图像掩饰面孔或报告结果作为汇总的统计资料,以确保他们不会确定一个具体的个人。

假名化涉及修改个人资料,使得仍然可以通过使用诸如ID号的独特标识符或散列算法来区分资料集中的个人,同时分别保存其个人资料用于检查目的(参见Q9)。

当采用这种技术时,调研人员应该咨询当地的国家法律和自律法规,以确定哪些要素必须被删除,以符合这些资料的匿名/假名法定标准。

7 来源和参考

[DLA Piper, Data Protection Laws of the World](#)

[EphMRA Adverse Event Reporting Guidelines 2014](#)

[ICC/ESOMAR International Code on Market and Social Research ESOMAR Interviewing Children and Young People Guideline](#)

[ISO 26362:2009 – Access panels in market, opinion, and social research Privacy Shield Framework](#)

[OECD 隐私原则](#)

8 项目团队

联席主席:

- Reg Baker, ESOMAR 专业标准委员会和国际营销调研所顾问
- GfK 完整性、合规性及隐私保护副总裁 David Stark

项目组成员:

- 市场调研学会首席运营官 Debrah Harding
- Stephen Jenke, 顾问
- ESOMAR 国际标准和公共事务部主任凯西·乔 (Kathy Joe)
- Wander Meijer, 全球首席运营官, MRops
- SSI 总法律顾问 Ashlin Quirk
- 全球隐私保护经理 - 美国运通项目, 政策和治理经理 Barry Ryan
- 瓦利斯咨询公司负责人 Jayne Van Souwe