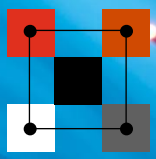
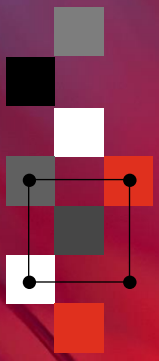
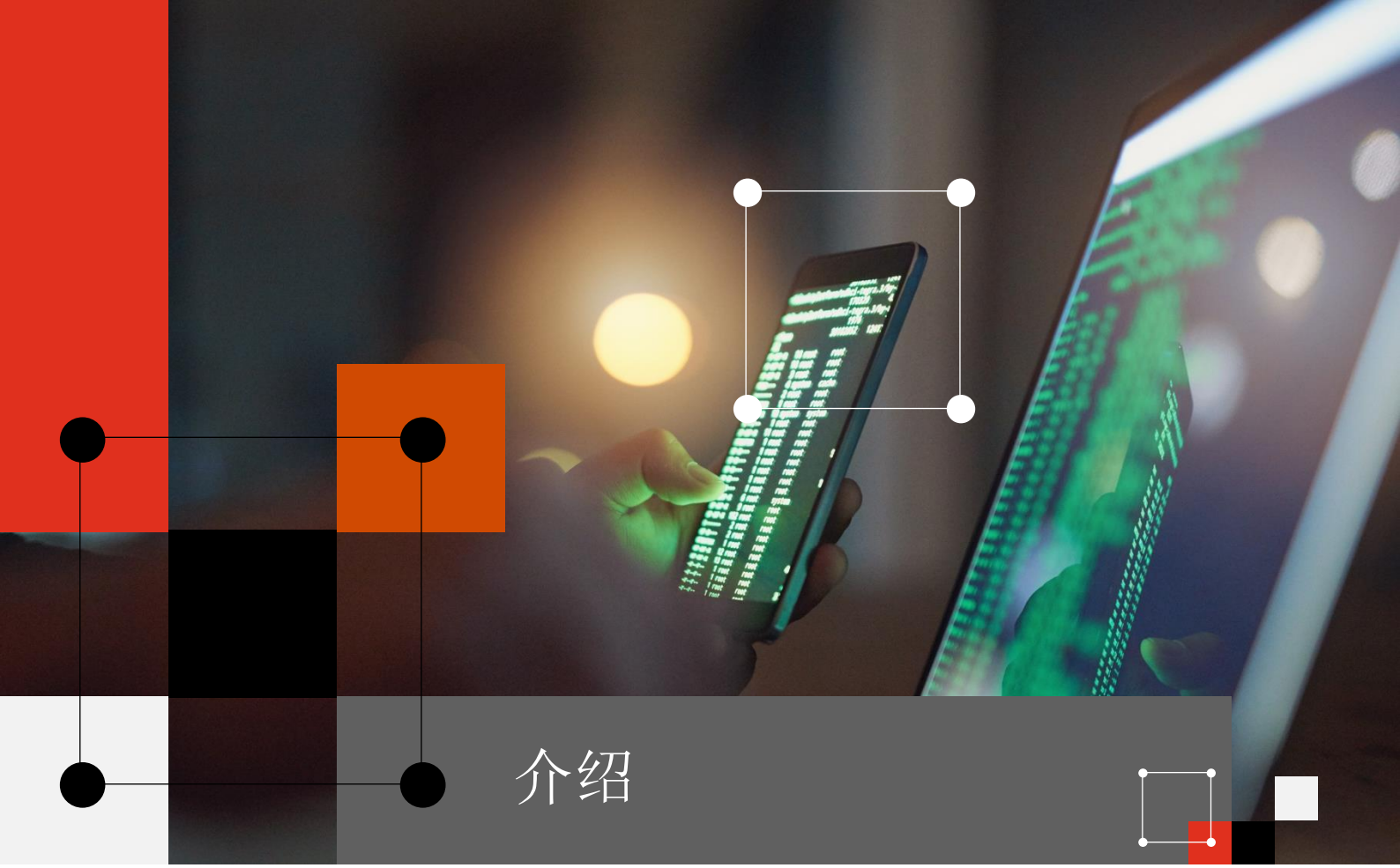
欧盟法规要求下的用户同意实践白皮书





pwc 普华永道

目录

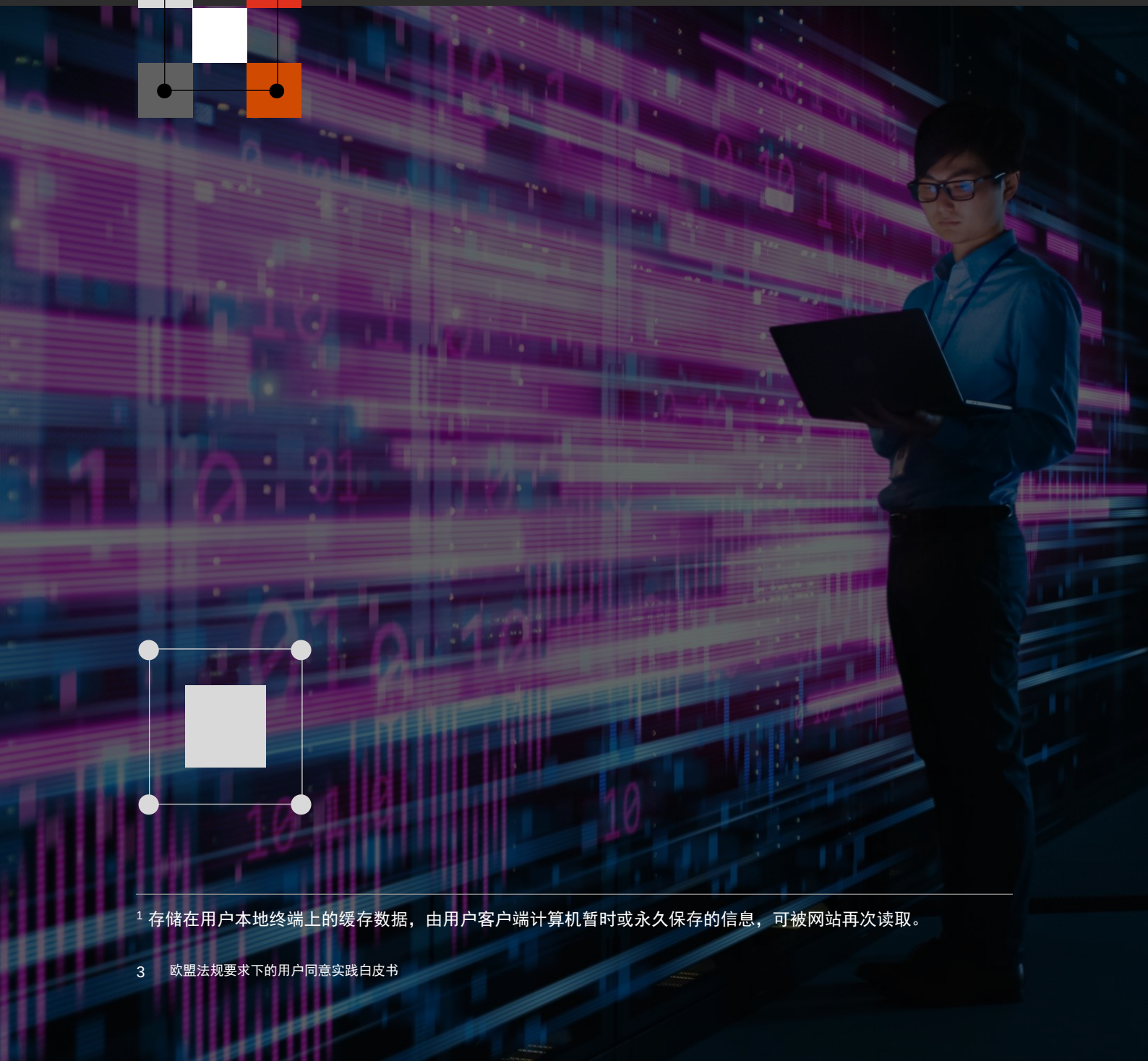


介绍

欧盟实施的《通用数据保护条例》(General Data Protect Regulation, GDPR)驱使全球数据保护法规更加严格，赋予了消费者更大的隐私权。随着GDPR执法模式的不断完善，在欧洲经济区（EEA）运营的公司必须遵守隐私保护法规，否则将可能面临高昂的罚款（罚款高达2000万欧元或上一个财年全球营业收入的4%），并且影响企业声誉，导致企业丧失消费者的信任。因此，企业应注意加强数据保护合规能力，以降低法律风险和经济风险，保障企业的可持续发展，同时可以赢得消费者的信任，打造良好的品牌形象，间接提高消费者对企业的忠诚度。

GDPR被公认为是隐私保护立法的重要里程碑，对数字广告行业产生了深远的影响。该法规限制企业收集和处理来自欧盟 IP 地址的个人数据。同样，英国脱欧后，《英国通用数据保护条例》（UK-GDPR）和《2018年数据保护法》也约束了企业作为网站或应用程序所有者必须获取和存储用户同意，即英国地区的企业也应遵守相同的要求。在处理个人数据之前，广告商和出版商必须获得用户明确的同意，而且用户可以随时撤回同意。因此，企业必须清楚了解自己的义务。本白皮书全面概述了欧盟关于获得“用户同意”的监管要求，并提供了良好实践的范例。

- 第1章对GDPR和ePrivacy Directive（《电子隐私指令》，ePD）有关用户同意的要求进行了介绍，其中包括与Cookie[1]或个性化广告等主题相关的案例研究和解释。
- 第2章提供了制作合规横幅的实用指导。
- 第3章列出了针对用户同意实践的常见问题以及答复。



[1] 存储在用户本地终端上的缓存数据，由用户客户端计算机暂时或永久保存的信息，可被网站再次读取。

第1章 GDPR和ePD针对用户同意对企业的要求

ePD规定了Cookie或类似技术的同意要求，而GDPR规定了有关个人数据处理活动同意的一般原则。欧洲数据保护委员会（EDPB）也在其《关于GDPR下“同意”》的指南中明确指出，GDPR下获得有效同意的条件也适用于ePD范围内的情况。因此，我们更关注GDPR的同意要求。根据GDPR的要求，处理个人数据必须具有法律依据。企业处理个人数据大多采用“获得数据主体[2]的同意”作为法律依据。根据GDPR的定义，个人数据是指与已识别或可识别的自然人（“数据主体”）有关的任何信息，如姓名、身份证号码、位置数据、在线标识符或与该自然人的身体、生理、遗传、心理、经济、文化或社会身份有关的一个或多个特定因素。总之，如果企业采用“用户同意”作为网站或应用程序处理个人数据的法律依据，则需要遵守以下有关用户同意的要求。

一 用户同意应当满足有效性

有效的用户同意是指，数据主体通过声明或明确肯定的行动来表示同意处理与其有关的个人数据，意思表示应当是自由给予的、具体的、知情的和明确的。应注意以下四个关键要素：

- **自由提供：**意味着数据主体拥有真正的选择权和控制权。对数据主体施加任何不适当的压力或影响阻止数据主体自由地行使其意愿，都会导致获取的同意无效。

  - 不能把同意作为服务条款的捆绑部分。

例：某网站提供商安装了一个脚本会阻止网站内容的显示，只显示询问是否同意Cookies的请求以及正在设置哪些Cookies和出于何种目的处理数据的信息。如果不点击“接受 Cookies”按钮，就无法访问内容。由于没有向数据主体提供真正的选择，获取的同意不是被用户根据自由意愿提供的。

[2] GDPR将数据主体定义为“已识别或可识别的自然人”，从其处或收集关于其的信息。

- 不应让用户一次性对多个处理目的提供同意，数据主体应可自由选择他们接受的目的。

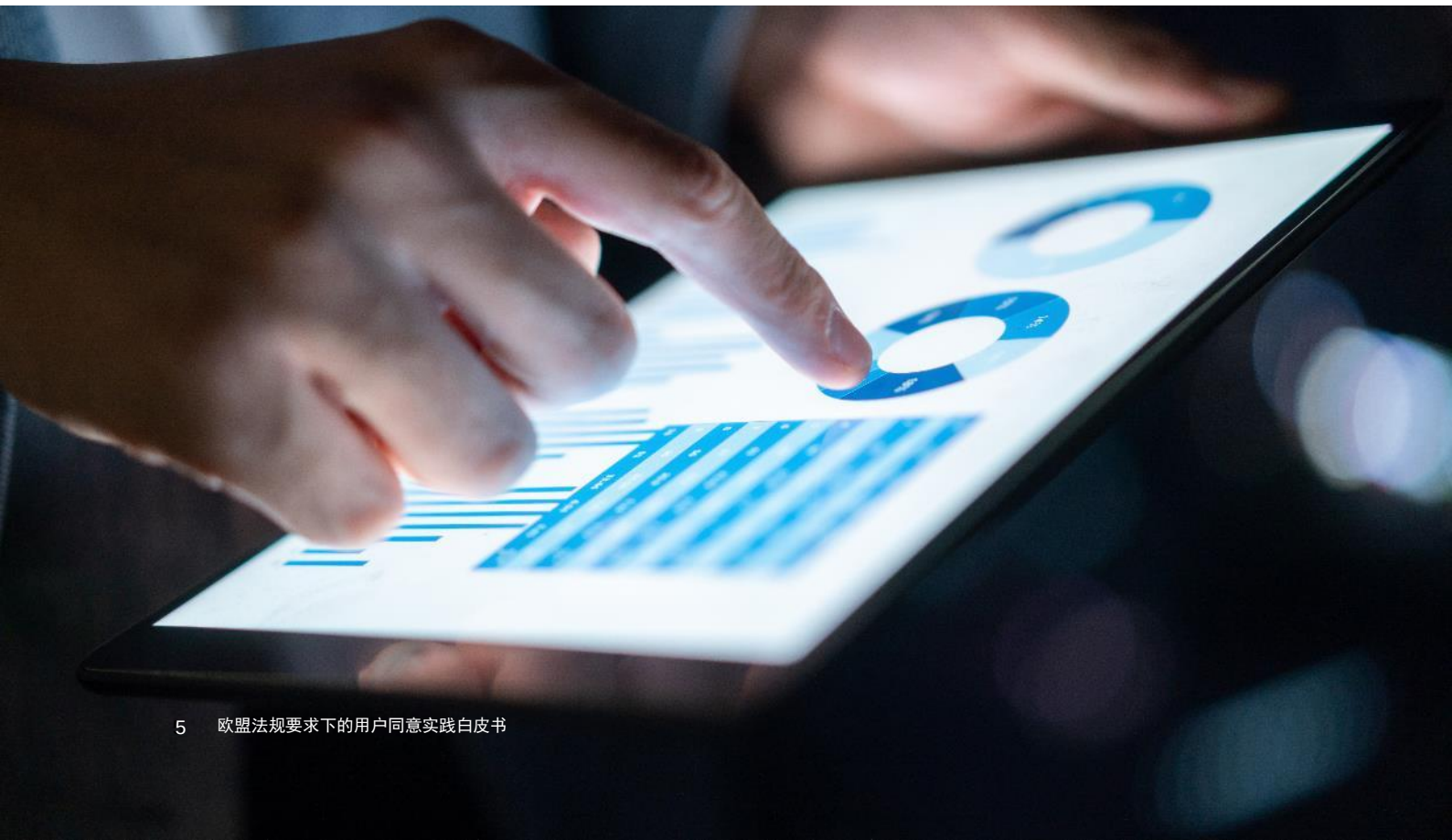
例：在同意请求中，零售商要求客户同意使用其数据通过电子邮件向其发送营销信息，并与集团内其他公司共享其详细信息。这种同意的范围比较宽泛，没有针对这两个不同的处理目的设置单独同意，因此这种同意无效。

- 拒绝或撤销同意不能对数据主体造成损害（如额外费用、服务性能下降）。

例：客户订阅了某时装零售商提供折扣的资讯，零售商要求客户同意收集更多有关购物偏好的数据，以便根据客户的购物记录或自愿填写的问卷，为其量身定制优惠。当顾客后来撤销同意时，仍应收到相同的折扣但不包含个性化营销资讯。

- **具体：**意味着确保用户数据对用户的透明度，用户对数据具有一定程度的控制能力。数据主体必须在对特定处理目的知情的情况下，始终对特定的处理目的表示同意。如果为各种不同的处理目的征求同意，应该为每种目的提供单独的选择，允许用户为每种特定目的给予特定同意，并告知每种目的的信息。

例：某游戏应用程序根据用户的同意收集他们的个人数据，并根据他们的操作习惯推荐用户可能感兴趣的游戏内容。一段时间后，该应用程序决定让第三方根据用户习惯发送（或显示）有针对性的广告。鉴于这一新的目的，则需要征得新的同意。



- **知情：**要求在征得数据主体同意之前向其提供有关信息，使其能够做出知情的决定。征得同意的要求应与其他事项明确区分开来，以易懂、易获取的形式展现，使用清晰明了的语言表达。如：此类信息不应只隐藏在向用户展示的一般条款中。

  为获得有效的用户同意，至少应提供以下信息：

  a. 控制者的身份；

  b. 征求同意的每项数据处理目的；

  c. 将收集和使用什么（类型）数据；

  d. 用户撤销同意的权利；

  e. 根据GDPR第22（2）（c）[3]条，在相关情况下，提供有关使用数据进行自动决策的信息；

  f. 由于缺乏欧盟委员会的充分性决定和适当的保障措施（如GDPR第46条[4]所述），数据传输可能存在的风险。

[3] GDPR第22（2）条要求：数据主体有权不接受仅基于自动处理（包括用户画像）的决定，除非有以下三种情况之一的法律依据：（a）为签订或履行数据主体与数据控制者之间的合同所必需；（b）经数据控制者所遵守的欧盟或成员国法律授权，且该法律还规定了适当措施以保障数据主体的权利和自由以及合法利益；或（c）基于数据主体的明确同意。

[4] GDPR第46条要求：在向第三国或国际组织传输个人数据之前，控制者或处理者应提供适当的保障措施。

- **明确表示意愿**：有效的同意需要用户通过声明或明确的肯定行动来表示。同意可以通过书面或（记录的）口头声明，包括电子方式收集。

  数据主体的沉默或不主动反馈以及仅仅继续使用服务，都不能被视为主动选择的表示，所以需要注意收集用户同意时，应当提供有利于用户反馈的界面，如提供按钮和默认不勾选的条件框。同样，接受一般条款不能被视为同意使用个人数据的明确肯定行动。在设计同意机制时，应让数据主体清楚明白其同意的行为代表什么，避免含糊不清，并确保同意的行为可以与其他行为区分开来。

例：当用户第一次访问某网站时，他们会被告知Cookie被用来收集他们的交互信息，用于改善用户浏览体验。通过点击“接受”按钮，用户可以有效地执行“明确的肯定行为”，同意进行处理。此外，还需要向用户提供一个“拒绝”按钮，当用户点击“拒绝”按钮时，将不再收集他们的交互信息。

二 应获得“明示”同意的情况

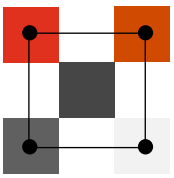
如果在下列情况下使用同意作为法律依据，则需要获取用户“明示”的同意，比常规同意的内容要求更严格：

- 处理GDPR第9条定义的特殊类别个人数据时，包括揭示种族或民族血统、政治观点、宗教或哲学信仰或工会会员身份的个人数据，以及处理基因数据、用于唯一识别自然人身份的生物特征数据、与健康有关的数据或与自然人的性生活或性取向有关的数据。

- 用于对个人数据的自动化决策的处理，包括用户画像[5]。

- 在缺乏适当保障措施的情况下向第三国或国际组织传输个人数据。

[5] 指任何形式的个人数据自动处理，包括使用个人数据对自然人的某些个人方面进行评估，特别是分析或预测该自然人的工作表现、经济状况、健康状况、个人偏好、兴趣、可靠性、行为、位置或行动。



如企业在处理用户个人信息时存在以上场景，普华永道建议咨询专业的第三方，对上述情况进行详细分析。

可以考虑通过以下方法之一获得数据主体的明确同意：

- 书面声明：数据主体通过提供书面声明明确表示同意，在适当情况下可能需要签名。
- 数字或在线同意：数据主体通过填写电子表格、发送电子邮件、上传带有数据主体签名的扫描文件或使用电子签名来表示同意。
- 分两阶段核实用户同意：可分两个阶段核实同意，以确保其真实性和有效性。

为了最大限度地避免合规问题，建议不要将特殊类别数据和精确位置数据用于广告目的的数据处理。

三 获得儿童同意的额外要求

在处理弱势自然人（尤其是儿童）的个人数据时，需要根据GDPR要求建立额外保护机制，特别是适用于为了营销或创建个性/用户档案而使用儿童个人数据，以及直接向儿童提供服务时收集儿童的个人数据。如果网站或应用程序以儿童为目标受众，则在基于同意进行数据处理时，应注意附加要求：

- 如果儿童未满16周岁（根据欧洲经济区各国的法律可能有所不同），只有在儿童的父母监护人同意或授权的情况下，此类处理才是合法的。
- 应考虑到现有技术，尽力核实同意是否由儿童的父母监护人给予或授权。

如果希望最大限度地避免合规问题，建议在业务中禁止针对儿童的个性化广告。

四 撤回同意的要求

GDPR第7（3）条规定，数据主体有权随时撤回其已提供的同意。有关撤回同意的一些具体要求如下：

- 数据主体应能够像提供同意一样方便地撤回其同意。例如，如果同意是通过网站或应用程序的特定服务用户界面获得的，则必须可以通过相同的电子界面撤回同意。
- 撤回同意应是免费的，且不会导致服务质量下降。
- 必须告知数据主体其具有撤回同意的权利，这是为获得有效同意而提供的信息的一部分。
- 如果数据主体撤回同意，必须立即停止数据处理。如果没有其他合法依据，则必须删除数据。

五 同意的记录

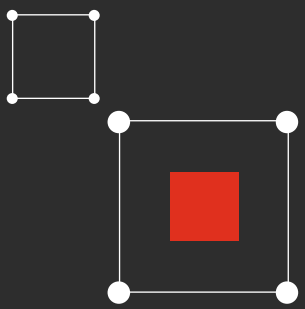
GDPR第7（1）条中，明确概述了控制者具有证明数据主体同意的明确义务。换句话说，企业应保存从数据主体处获得同意的记录。只要相关数据处理活动持续进行，企业就有义务证明曾获得用户同意。而处理活动结束后，同意证明的保存时间不得超过履行法律义务或确立、行使或捍卫法律主张所严格需要的时间。

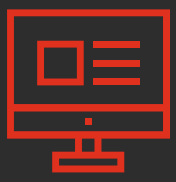
第2章 在欧洲经济区建立合规横幅的最佳实践

一 网站同意横幅的注意事项

步骤1：了解用户同意方面的监管要求

可以参考第1章有关欧洲经济区和英国关于用户同意的要求。请注意，它们是通用要求，还需要了解其他可能存在的差异（例如，儿童的年龄的定义）。





步骤2：审计网站所使用的技术，识别Cookie和其他跟踪器

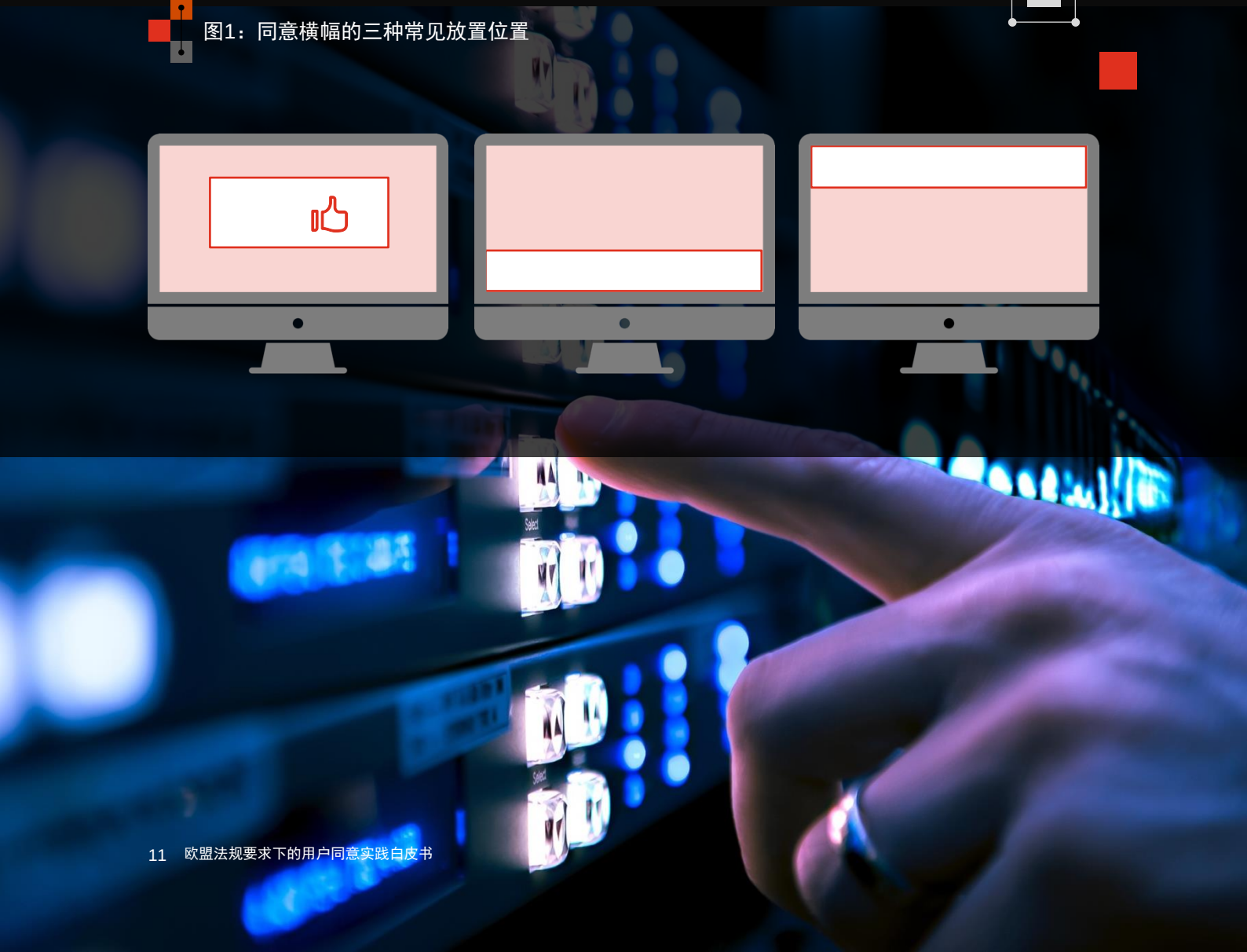
对网站进行全面、彻底的扫描，了解网站上的Cookie、信标和其他跟踪技术。验证Cookie的使用是否符合网站隐私政策或放置Cookie的第三方网站的隐私政策。对网站进行审计可以自动检测和分类Cookie等跟踪技术，有助于消费者理解并选择正确的内容。Cookie通常有以下几种类型：严格必要的、功能性的、统计性的、营销性的等。只有严格必要的Cookie可以默示同意，其他类型的Cookie应由用户自主选择接受或拒绝。步骤3将对此作进一步解释。

步骤3：设计横幅

当设计同意横幅时，建议充分考虑以下内容。这些内容可以提升用户友好体验，可能会增加用户同意率。其他要求应以当地数据保护机构发布的指南为基础，在一些同意管理平台上也可以找到相关指南。普华永道在此提供一些实践做法供参考。

- 位置：横幅的位置是影响同意率的关键因素。常见的放置位置包括在网页的中间、网站的页脚和网页的顶部。将横幅置于中间位置往往能吸引更多的注意力。业内调研曾发现放置在页面中间的同意横幅获得了最高的同意率。

图1：同意横幅的三种常见放置位置



- 内容：需要充分考虑用户同意方面的合规要求，如第1章所述。应当以简单易懂、不使用过于专业晦涩的语言告知用户有关Cookie使用的信息，信息应包括：

  a) 明确标识组织名称。在横幅上显示所在的组织名称或徽标；如果网站将与第三方（如广告或分析合作伙伴）共享通过Cookie收集的数据，同意横幅应告知用户此类数据共享做法；

  b) 说明将收集和使用哪些（类型）数据；

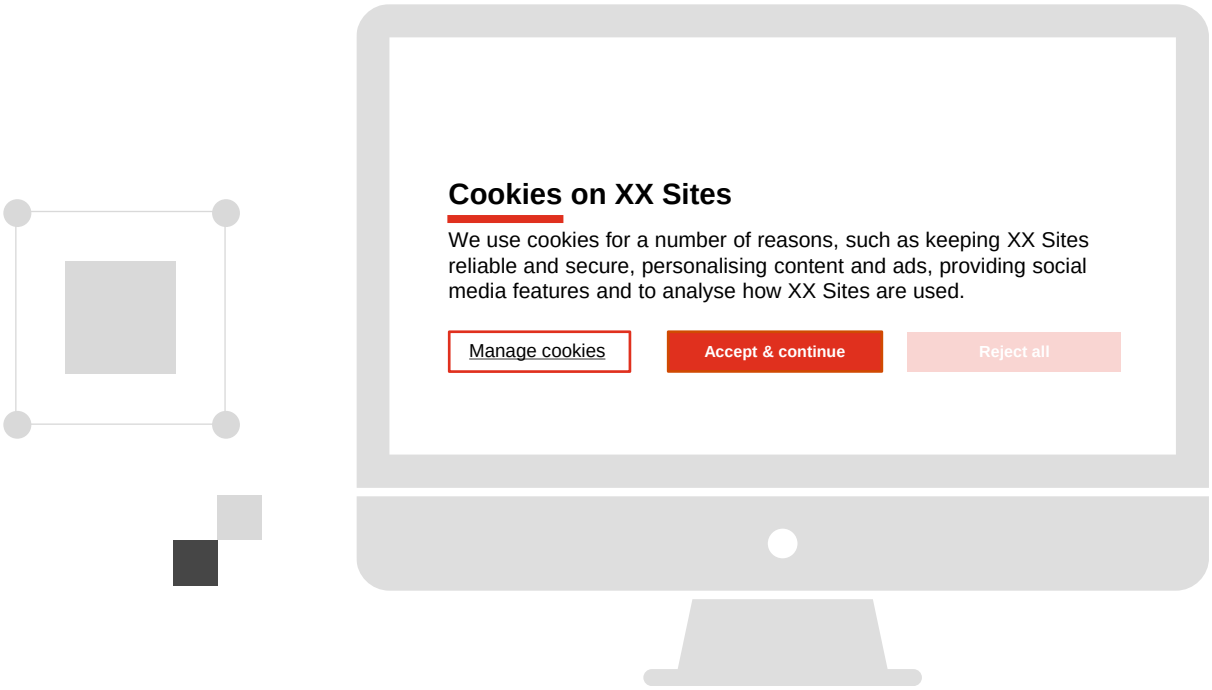
  c) 解释收集数据的原因（处理的目的）。例如，使用Cookie收集到的数据为用户提供相关促销（营销）信息，或是提供更好的网站体验（功能）；

  d) 告知用户随时撤销同意的权利以及撤销同意的方法；

  e) 指向网站详细的Cookie政策和隐私政策的链接。还建议横幅上提供一个链接，展示共享数据的供应商列表。

- 按钮：在横幅上应清晰地显示“接受”和“拒绝”或类似含义的按钮。只有用户主动点击“接受”按钮才能被视为有效的同意。研究表明“接受+拒绝”这种按钮组合的同意率较低，因为如果用户不了解正在发生的事情，他们通常会选择拒绝。相比之下，“接受+设置”组合会获得最高的接受率。还可以通过让人愉快或信任的语气增加用户的同意。例如，“请接受！”和“【网站名称】重视您的隐私”的方式，以不同程度增加用户的接受率。

图2：同意横幅按钮的做法*



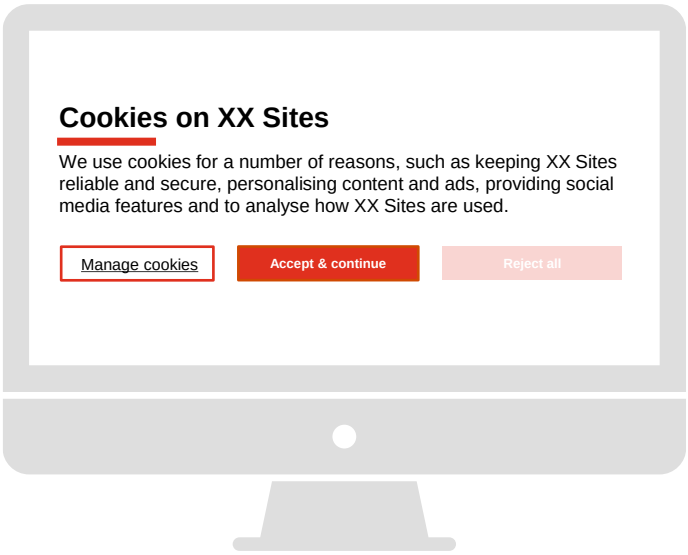
* EEA地区英语界面示例

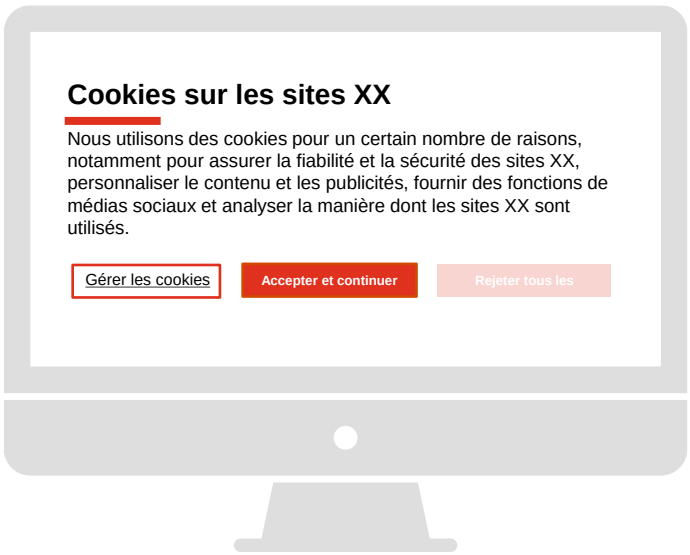
- 颜色：可以根据组织的形象与风格，设计同意横幅的颜色。在字体颜色方面，尝试视觉冲击强的颜色搭配（例如深色背景和亮色文本，而不是亮色背景和深色文本），可能会提高同意率。例如，“拒绝”按钮使用浅色，“接受”按钮使用较深的颜色，有边框，且有一个易于选择的图标。

- 字体：通常标题文本设置字体（例如组织名称和按钮文本）应足够大，便于查看；描述信息收集目的的文本一般以较小的字体显示，长度不宜过长或过短；隐私政策和Cookie政策的链接应通过不同的字体（例如斜体、粗体等）和颜色来区分。

- 语言：根据网站所在的国家或司法管辖区，显示本地语言的横幅，让用户有效地理解内容。

图3：不同语言横幅显示的实践参考*





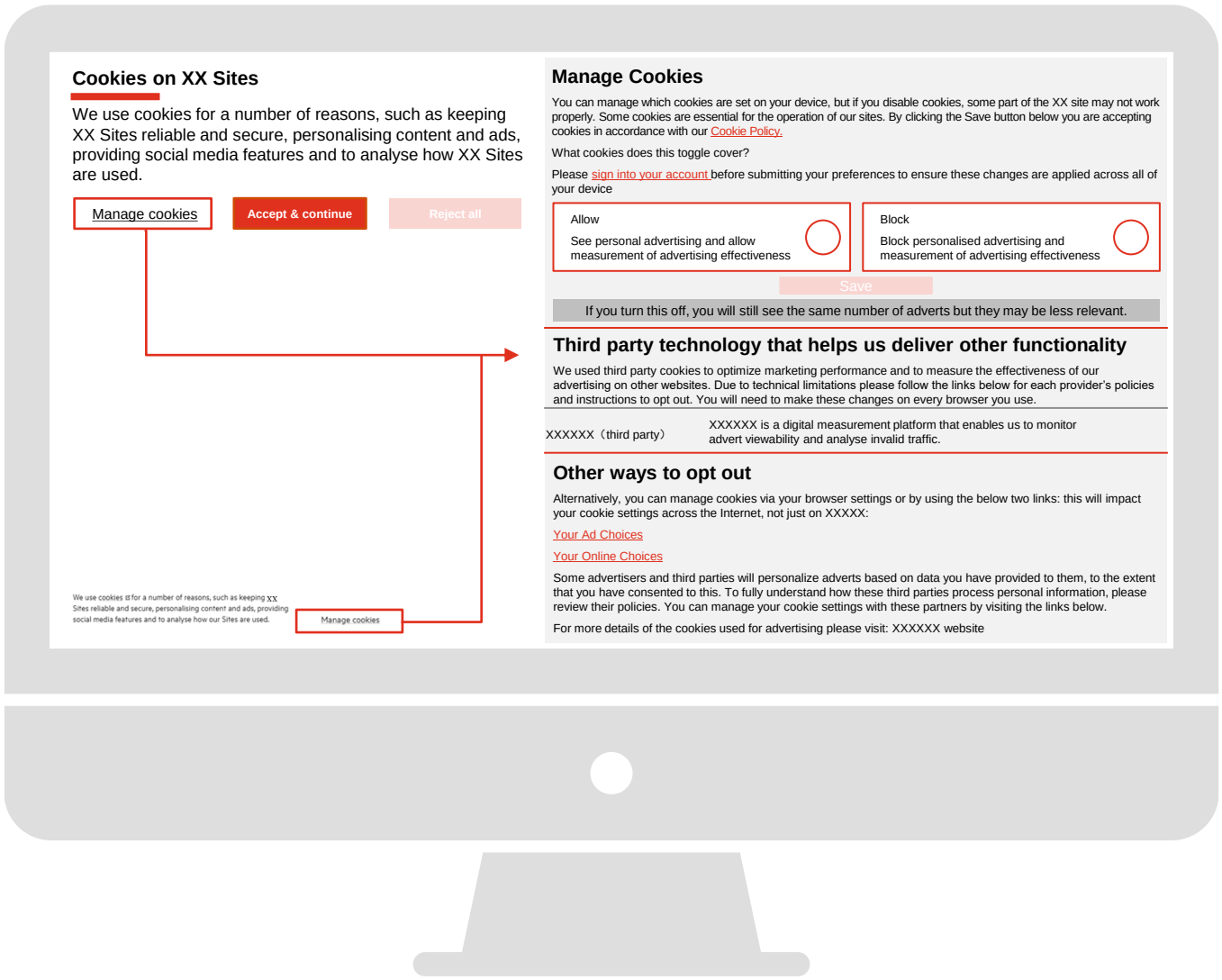
* EEA地区英语、法语界面示例

- 同意管理机制：

  a) 在同意横幅之后，用户可通过“管理Cookies”按钮或链接进入同意管理界面。在收集用户个人信息之前，应向用户提供选择权来选择他们希望接受的Cookie选项。如步骤2所述，对Cookies进行分类，并告知用户各类Cookies的作用。除严格必要的Cookies外，所有其他类型的Cookies都需要用户主动勾选。

  b) 还应该具备明确简单的退出机制，让用户能够随时撤回他们的同意。通常可以在网页页脚提供用户管理Cookie的链接，在弹出的Cookie横幅后，用户可以通过简单的方式进入网页来管理Cookie，例如更改同意偏好。

图4：同意管理机制的实践参考*



* EEA地区英语界面示例

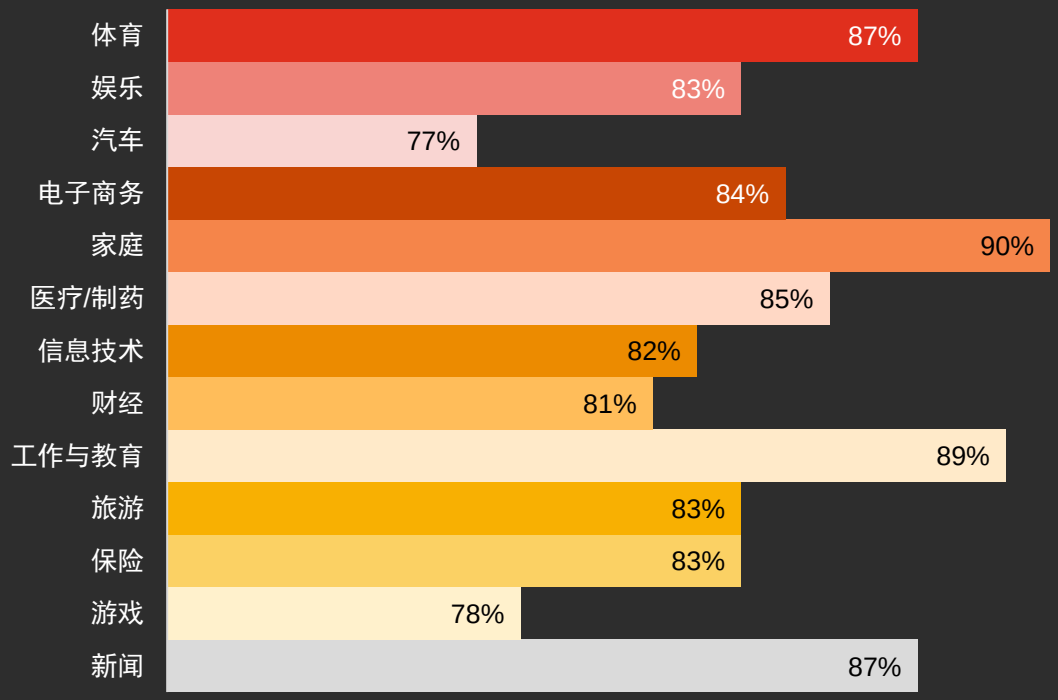
步骤4：仔细检查

应该确保在获得用户同意之前阻止网站跟踪器的自动运行。确保横幅设置和Cookie执行方式与呈现Cookie和隐私政策一致。在正确的时间，向正确的人显示正确的同意横幅。

步骤5：衡量同意率

在网站上有了基本的横幅之后，监控同意率也很重要。如果选择同意的人数较少，可以选择一些第三方平台对同意率进行一些测试。通过A/B测试、实验，和对模板设计、布局、文本、行动呼吁按钮（CTA）、颜色等简单测试，确定哪些变化产生了最高的转化率。根据一些同意管理平台的实践，同意率在不同行业之间变化很大。

图5：主要行业的同意率[6]

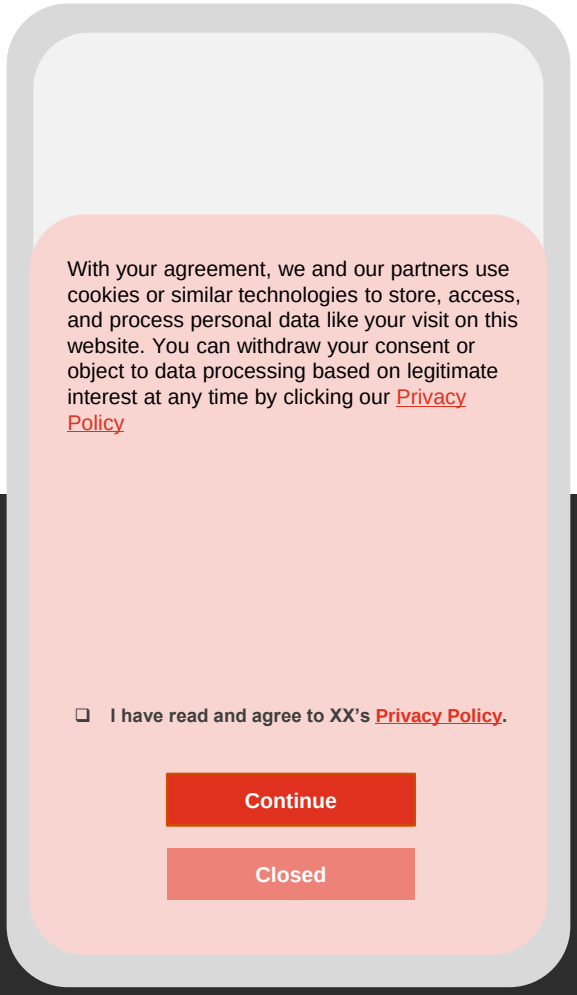


[6] 来源：Consent Manager对使用其CMP平台的15,000个网站的10亿多个同意层的统计分析结果

二 应用程序同意横幅的注意事项

应用程序端的同意因业务的多样性更为复杂，在此仅提供一些一般性建议供参考。进一步的指导应参考应用程序发布平台对开发者的要求，如Google Play的指南或Apple App Store的指南。在进行开发之前就开始考虑隐私设计（Privacy by Design）也很关键。

图6：移动程序端网站的实践参考*



步骤1：了解有关用户同意的监管要求

对于应用程序提供者而言，在欧洲经济区和英国发布应用程序需要遵守的监管要求与第1章所述要求相同。此外，还需要遵守发布应用程序的应用平台的隐私政策。

步骤2：审核应用程序中的服务和应用程序接口（API）是否合规

在集成第三方服务或API时，应考虑GDPR的要求，对应用程序进行彻底扫描。第三方服务或API的详细信息需要展示在网站隐私政策中。

* EEA地区英语界面示例

步骤3：在应用程序上设计并设置同意横幅或同意框

如果选择“获得数据主体的同意”作为在应用程序上处理数据的法律依据，则应在首次处理数据前征得用户同意。建议采用符合GDPR的唯一方法——在应用程序启动时显示同意横幅（横幅、框等形式）。

在iOS设备上提供应用程序时，还须遵守苹果对应用程序开发人员的要求：在符合各地法规要求获取用户同意之外，单独获得用户对应用程序跟踪透明度（ATT）[7]的同意。

与网站上的同意横幅一样，需要对内容、按钮、颜色、字体和语言进行类似的设置。（此处不再赘述）。

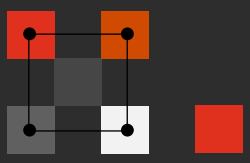
- 位置：建议将应用程序弹出窗口放在屏幕的中部或下部，这样更容易吸引用户的注意力，也方便用户点击。

- 同意管理机制：

a) 可以选择侧边栏或菜单项链接到管理隐私和数据收集的界面。向用户展示隐私政策、所收集数据类型的相关信息，并允许用户更改同意选择。此外，还应在设置页面上为用户提供是否启用个性化广告的选项。

b) 同样，符合GDPR标准的移动应用程序也应该有专门的页面，让用户可以选择退出与应用程序的通信或要求删除他们的数据。该页面的入口应简单明了。

c) 此外，有必要实施GDPR要求的其他合规措施，如为数据主体提供行使其权利的机制。建议咨询专业的第三方机构，以获得有关更多情况的详细分析。



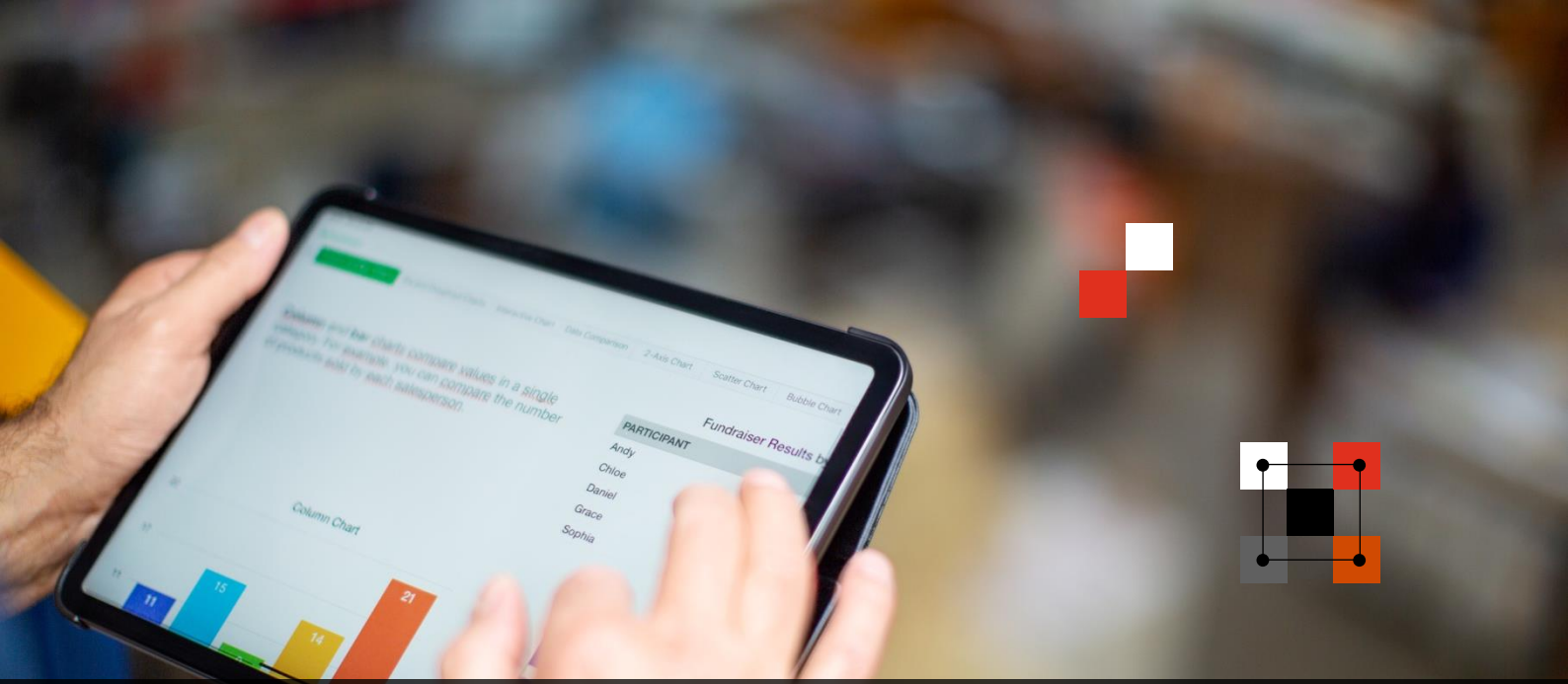
[7] 在iOS设备中，需要通过应用程序跟踪透明度（ATT）框架获得用户许可，才能跟踪用户或访问其设备的广告标识符。更多信息，请参阅Apple。

步骤4：仔细检查

在获得用户同意之前，应用程序不能采集用户信息。确保应用程序的数据收集方式符合隐私政策。

步骤5：衡量同意率

最后，还需要监控应用程序的同意率，并使用合适的方法进行测试，以找到促进积极效果的变化方向。



三 合规的同意横幅的检查清单

以下检查清单提供设计同意横幅时应当避免的常见错误。

- 针对来自欧洲经济区（EEA）的用户访问您的网站或应用程序的场景，您是否检查了同意横幅的显示情况？
- 在获得用户同意之前，您是否禁止了网站跟踪器等技术自动运行？
- 当用户同意在您的网站或应用程序上被收集个人数据时，您是否向用户清晰说明收集哪些种类的个人数据，及收集数据的原因？（例如，他们是否知道他们的个人数据将用于个性化广告？）
- 您是否告知用户，使用其数据的组织或机构（包括第三方）以及使用数据的时间？
- 您是否为每个数据处理目的提供了单独的同意选项，而不是将同意捆绑以涵盖多种目的或活动？
- 用户是否可以通过点击“确定”按钮或“我同意”按钮等清晰积极的操作来表示同意？
- 您是否为用户提供了便捷的途径，供用户修改其同意偏好或撤销同意？
- 在获得用户同意后，您是否记录并保存了这些同意数据，以便在数据保护机构（DPA）进行审计时用于验证用户的同意？

第3章 Q&A

在横幅上可以只提供一个“接受”按钮吗？

根据GDPR的规定，需要为用户提供选择退出的选项。可以同时提供“接受”和“拒绝”按钮，或者只提供“接受”按钮，但应当允许用户进入管理Cookie页面设置Cookie偏好。

如果不允许用户在不同意的情况下使用游戏服务会怎么样？

同意必须由用户“自由给予”才有效，这意味着同意处理个人数据（非履行合同或服务所必需的）不能与该合同或服务的提供相绑定。因此，不建议将提供基本服务目的（玩游戏）与广告目的相绑定使用户的同意一起做出。

需要展示所有第三方的信息吗？

是的，在GDPR下，应该包括所有与之共享用户信息的第三方供应商，并清楚地链接它们的数据政策。

如果用户拒绝，多久可以再次弹出同意横幅？

在法律上，当用户不同意时，不应记录该用户的任何信息，您不会感知到用户拒绝了同意后再次访问，所以应该将未同意的用户视为新访客。

是否可以将同意声明包含在条款和条件声明中？

将同意声明与条款和条件结合在一起通常会导致文档冗长复杂，难以阅读。建议单独提供同意声明，以便用户更清楚地了解他们的数据将如何使用，并明确表示同意。

结论

在数字化飞速发展的当下，数据保护监管机构实施的法规愈发严格，企业在数据合规方面面临着很大的挑战。本白皮书介绍了欧洲经济区有关用户同意的法规要求，提供了良好做法的范例，并就如何降低合规风险提供了指导。企业可以参考本白皮书，了解有关用户同意的欧洲经济区法规介绍和良好实践范例，并采取相应措施降低合规风险。

联系我们

汪颖

普华永道中国法务数字化管理与战略咨询服务主管合伙人

jane.y.wang@cn.pwc.com

周晓琴

普华永道中国法务数字化管理与战略咨询服务合伙人

elle.zhou@cn.pwc.com

叶天斌

普华永道中国数字化与科技咨询服务合伙人

tianbin.ye@cn.pwc.com