COOKIE合规指引（2021）

2021年3月

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

版权声明

编写团队

编写单位：

北京市环球律师事务所

小米集团

编写组成员：（姓氏笔画为序）

朱玲凤、杨汉轩、张淑怡、孟洁、殷坤、徐晨、钱星辰

联系人：

孟洁

电话：010-65846768

邮箱：mengjie@glo.com.cn

目 录

图目录

前 言

在 PC 互联时代，基于网页诞生的 Cookie 及相关类似技术（如 Local Storage）等，在实现网页通讯、验证客户端身份、免去用户重复登录并记录用户的偏好设置上起到了重要的作用，提升了用户网页浏览和使用的体验。但是，又因 Cookie 能够识别客户端以及在登录情况下识别用户，天然具备了追踪用户的技术优势，从而可能追踪用户的浏览、点击行为，进而该技术被用于形成用户画像、预测行为、推送营销广告等目的。由此应运而生了第三方统计公司、第三方营销公司，使用第三方 Cookie 的机制，读取并融合同一用户在不同网站上的行为，对用户的个人数据引发了大量的风险和损害，引起广泛讨论。

因此，各国对于 Cookie 及类似追踪技术都应运而生相应的法律规制。近期因广告追踪问题，第三方广告营销公司频繁被监管机关调查乃至于受到高额处罚。从 2019 年底开始，欧盟地区与 Cookie 相关的执法案例也逐渐增多。比利时、法国、西班牙等各国的数据保护监管机构都纷纷针对违规使用 Cookie 的行为开出罚单。尤其是法国数据保护监管机构 CNIL 于 2020 年 12 月对于 Google 和 Amazon 违法使用 Cookie 的行为分别处以 1 亿欧元和 3500 万欧元的巨额罚款，再一次引起了全球对于 Cookie 的关注。

故本合规指引报告由环球律师事务所和小米集团数据合规团队共同编撰，以厘清 Cookie 的主要问题、提供广泛的多法域对 Cookie 的规制以及行业实践，为数据合规行业的同仁提供参考。

本合规指引报告前三章对 Cookie 及相关追踪技术进行了详细的介绍，有助于读者更好地理解 Cookie 及类似技术的工作机制和原理。尤其是阐释了第三方 Cookie 的运作机制以及使用背后所产生的隐私担忧。

第四章指出了 Cookie 违规使用频繁被查的背景，也引出互联网企业针对 Cookie 合规工作的重要性。第五章至第六章详细梳理了欧盟、美国与我国在法律规定上对 Cookie 是如何规制的以及已发生的重点案例，对不同国家或地区的 Cookie 合规要求进一步提供了指引。

欧盟明确对 Cookie 机制予以规制的规定最早出现于 2002 年《电子隐私指令》，要求在按照《数据保护指令（95/46/EC）》充分告知用户关于 Cookie 的全面信息，且给予用户拒绝的权利后，方可在终端设备上存储或访问 Cookie 的信息。2009 年修订后的《电子隐私指令》将 Cookie 的合规要求从 Opt-out 改为 Opt-in，即从告知和拒绝权改为了需要经过用户同意方可存储和访问 Cookie。第 29 条工作组在后续的相关指引中明确了同意的具体条件以及可豁免同意的 Cookie 类型。关于 Cookie 同意的条件，在 GDPR 生效后，要求适用于 GDPR 关于同意的严格要求，即须符合通过声明或肯定的行为、自由作出、具体、知情且明确的同意。而《电子隐私指令》从法律性质而言是欧盟层面的指令，不得直接适用于欧盟各国，需要转化为国内法适用，这会导致各国在具体规定和执法上产生差异。各国为了更好地推动本国企业合规，还制定了各自的 Cookie 指引，包括德国、法国、希腊、英国等，相互之间存在共性与差异。本指引报告对上述四国的 Cookie

指引做了详尽的对比分析，以提供有意义的参考。而该差异化有可能因欧盟最新《电子隐私条例》的出台而一定程度的终结，故本指引报告也将《电子隐私条例》（欧盟理事会通过版）关于 Cookie 的规制进行了分析。譬如，其增加了对用户隐私侵害小的 Cookie 豁免同意类型，也鼓励采用更合理的同意机制，包括考虑通过软件设置、同意基于特定目的将一个或多个服务提供者加入白名单，以表示同意其使用某些类型的 Cookie，来解决频繁同意请求导致同意实质无效等。

美国虽然没有专门针对 Cookie 的法案或者具体法律条文，但是并非对于 Cookie 的使用没有任何规制。《儿童在线隐私保护法》、《加州在线隐私保护法案》等相关法律分别在联邦层面和州层面提出了针对 Cookie 及类似技术使用相关的规定，以规范企业对于在线追踪技术的使用，保障用户相关权益。值得关注的是 CCPA 和 CPRA 将 Cookie 纳入到在线标识符，明确了要求告知用户的义务以及赋予包括知情权、删除权、更正权、退出权等用户权利。但是总体而言，除了特殊人群外，美国基本上采取 Opt-out 的规制机制。

我国目前法律体系中虽然暂时也没有对于 Cookie 及类似追踪技术进行直接明确的针对性规定，但是因 Cookie 具备识别性，应当纳入到个人信息保护范畴，故应受到《民法典》、《网络安全法》等规制。而《个人信息保护法（草案）》在同意之外提供了其他合法性基础，可能对于 Cookie 的同意豁免有了适用空间，而且对于第三方的“单独同意”可能会影响第三方 Cookie 的合规要求，需要进一步关注《个人信息保护法（草案）》的进一步发展。

本合规指引报告在第七章展示了若干国内外网站具有代表性的 Cookie 合规实践做法，并依照各国的相关规定详解了各个部分的依据和实际意义，以可视化的形式，结合具体产品交互，解读法律文本中的相关要求，以增强落地实践性。

此外，随着 Cookie 在实践当中遇到的越来越多包括法律规定和监管在内的障碍，同时也为了更充分地保护用户隐私和个人数据相关权利，一些机构或企业试图通过技术来解决 Cookie 机制带来的隐私担忧。比如，2010 年提出的“Do Not Track“理念，将用户不希望被追踪的意愿告知给第三方公司，目前浏览器基本均支持该功能。再比如，2019 年谷歌提出了隐私沙盒机制，以更缓和的方式替代 Cookie 实现跨站点追踪功能，并且提供给用户更方便关闭的途径等。以及结合数据保护设计等理念，采取的”the 5th Cookie“和联邦学习等机制，尽可能地淡化定位到单独唯一的个人。本章对这些相关内容也有说明，以帮助读者了解 Cookie 及类似技术的发展趋势，和未来在这一领域可能或已经出现的技术和法律规定上的进展，使企业有所准备。

最后，本合规指引报告综合以上对于各地法律规定、实践指南的要求，结合具体监管处罚的重点和要点，分别向国内网站运营者和有出海业务的国内企业提出了有针对性的 Cookie 合规具体建议。希望能够帮助有相关需求的企业在使用 Cookie 等类似追踪技术时防范风险，切实重视和保护用户的隐私，提升企业品牌形象，营造良好的市场氛围和合规环境，促进行业的创新和持续发展。

一、什么是 Cookie，以及第一方 Cookie 的产生缘由

Cookie 一般是指当用户浏览或访问网站或其他网络内容时，网站服务器存放在用户本地设备（例如电脑、移动电话或其他设备）内的载有一连串文字的小型文本文件（主要由名称、域、路径、失效时间、安全标志等部分组成，可以存储用户 ID、密码、浏览过的网页、停留的时间等用户身份信息和浏览记录）。Cookie 最早出现于 20 世纪 90 年代，其产生时的目的是为了解决用于互联网浏览器和服务器间进行通信传输的 HTTP 协议不能表示状态从而无法判断客户端身份的问题。因此，程序员在技术层面，通过在 HTTP 头部放置一些服务器生成的字符串（即 Cookie），使浏览器端在收到后进行保存，且在之后每次请求 HTTP 协议时都带上 Cookie 的请求头，服务器验证了 Cookie 值后即能够判断浏览器发送的请求是来自于哪个用户。[1]

Cookie 按照其功能，主要分为两类：一类支持网站运行功能，丰富用户的使用体验，为用户的正常页面访问提供基础支持；另一类记录用户在网页浏览时作出的选择及活动轨迹，可用于不针对于用户个人的统计分析使用，便于提升网站整体的体验，也可用于分析用户的喜好、预测行动等，形成用户画像，为后续广告营销等活动提供便利。根据其使

[1] 参见 https://www.jianshu.com/p/f6606172b83b，最后访问日期 2021 年 2 月 18 日。

用目的的不同，Cookie 又可被分为基本类 Cookie、分析类 Cookie[2]、营销类 Cookie[3]和偏好类 Cookie[4]等。在用户客户端，Cookie 一般是基于浏览器进行管理的。通过对 Cookie 中“域（domain）”的部分进行设定[5]，同一个域名下两个二级域名可以使用相同的 Cookie，也可以使用不同的 Cookie ;但不同域名间 ,Cookie 通常无法跨越(典型特征), 不管是否因浏览器策略不同 Cookie 的运行和存储方式可能有所差异。例如，网站 A 会向用户客户端颁发 Cookie，而网站 B 也会向用户客户端颁发 Cookie，但网站 A 不能操作网站 B 向客户端颁发的 Cookie，而只能操作自身颁发的 Cookie。不同网站不能对非自身颁发的 Cookie 进行操作，Cookie 存储的文件只能被同一个域内的网页所读取，当文件未被分享和窃取的情况下，该 Cookie 存储的用户信息不会被该网页服务方之外的其他方获取。因此 ,能对用户隐私实现一定程度上的保护。

[2] 分析类 Cookie 一般用于收集网站运营情况相关的数据，如访客数量、页面和链接的点击情况等，以便改善网站的设计和功能、优化用户体验等。

[3] 营销类 Cookie 能够跟踪用户的在线活动，以帮助广告商衡量广告效果、建立用户画像并投放个性化广告。

[4] 偏好类 Cookie 有时也被称作功能性 Cookie，此类 Cookie 可以记录用户在浏览该网站时进行的偏好选择，比如网站语言、展示的内容等，以提高用户的浏览效率并改善体验。

[5] 默认情况下 Cookie 在当前域下有效，也可以设置该值来确保对其子域是否有效。

二、什么是第三方 Cookie，及 Tracking 技术与隐私保护关系

许多互联网网站通过长期培育用户，已经拥有了庞大的用户基数，但由于新产品盈利模式匮乏，将流量转化为收入是这些网站一直以来的难题。广告投放成为了其中最主要的一个解决方案，Google，Facebook，YouTube 等网站都是通过向不同用户投放不同广告的方式，将自己的用户和流量资源转化为实际可变现的营收。广告收益最大化的基础之一是对用户有足够多的了解，因此，对用户进行 tracking（追踪）的技术开始普及。在线广告公司创建了他们的特定用户访问了哪些网站的详细资料，以便将广告和优惠定位到该用户。例如，网站运营企业能准确追踪用户长时间在互联网上访问了哪些页面，做了哪些感兴趣的事情，从而推断出该用户一般类别的兴趣到潜在的详细个人信息。从技术层面上讲，一家网站运营企业可获取的用户信息几乎是无限的。[6]

为了更加广泛地实现这一目的，网站开始试图分享 Cookie 中存储的用户信息。相较于“第一方 Cookie”[7]，“第三方 Cookie”[8]的概念

[6] IAPP_T_TB_Introduction-to-Privacy-for-Technology_1.1

[7] 即前文所述的，由网络用户访问域所创建的 Cookie，通常是为了实现网站的正常功能和优化网站性能。

[8] 第三方 Cookie 指的是非访问站点所产生的 Cookie，可能在访问过程中加载了第三方的跟踪代码和资源，由第三方站点所产生的 Cookie。第三方 Cookie 一般由广告网络设置，用来“记住”其他时间的用户信息、在其他网站上向用户展示广告。第三方 Cookie 会在没有任何技术

屡被提及。第三方 Cookie 是指网站所有者外的第三方，比如 Google Analytics 这样的广告营销公司提供技术工具，帮助网站所有方获取用户与该站进行信息访问互动的 Cookie[9]，从而使个性化页面和定向广告解决方案落地。第三方 Cookie 在很长一段时间内都成为了 Google 在 PC 端广告业务方面的利器，通过第三方 Cookie，Google 大约能追踪 70%浏览量超 100 万的网站。[10]

那么，Tracking 技术与隐私保护有什么关系呢？从以下三方面解释说明。

第一，部分第一方 Cookie 和第三方 Cookie 有记录用户浏览轨迹等以提升网站服务的功能，因此很容易引起隐私保护的相关问题。

第二，有关第三方 Cookie 的其他细节，如 Cookie 的期限（在浏览器或客户端保留的时间长度）、获取方式（用户是否知情并获得同意）和是否有效执行“同源策略”（如前所述，只有同协议、同域名、同端口的同源网页方可获取相同的 Cookie），都和突破本网站并获取、追踪用

手段控制后续数据使用的情况下，向数百个市场参与者披露识别性数据，因此，通常认为，第三方 Cookie 并不是尊重隐私的技术。

[9] 参见 https://mp.weixin.qq.com/s/jlisBE5y6wCcyFsjq4WAcw，最后访问日期 2021 年 2 月 18 日。

[10] 参见 https://www.cookiebot.com/en/tracking-cookies，最后访问日期 2021 年 2 月 25 日。

户的个人信息关系密切。

第三，用于 Tracking 的 Cookie 文件安全性也无法得到有效保障。一旦 Cookie 被其他第三方获取，将会使用户遭受直接或间接的损失。此处，将通过介绍一个典型的 Cookie 使用场景来说明。例如，用户长期登录某特定的网页，必然希望避免每次登录时从第一页开始一页页地进入到最后访问页面，而是可以直接到达。因此，网页就将该用户登录的相关信息（如账号、密码等）保存在 Cookie 中，并设定一个较长的保存期限。用户在设定的期限内再次访问相同网站时，存储在浏览器中的 Cookie 登录信息被服务器验证，因此可免去重复登录的步骤。这种方式虽然便捷，但也给用户带来了安全问题和隐私泄露的隐患。一旦 Cookie 文件被该用户以外的其他第三方获取了，便可以冒充该用户使用其账户权限访问相应网站。而且，Cookie 中被读取的用户登录信息还可能与此用户的其他信息相结合，使用户身份在网页访问外的其他场景（如支付场景）中被冒用，造成更大的损失。虽然，技术上可以通过设置代码增强网站的安全性并对存储的信息进行加密等处理，但 Cookie 的整体安全性还是较低的。

三、用于用户追踪的其他传统技术

虽然上述说明了 Cookie 属性和作用，但它并不是目前用于认证身

份和追踪用户行为和喜好的唯一选择。并且在应用时，本身也存在一些问题和限制，如对移动端的支持不够友好，同源策略会导致应用受限等问题。为解决 Cookie 因其特性产生的短板，类似追踪技术也得到了较广泛的应用。

比较常见的有 Session 机制（基于 Cookie 的升级认证方式）和 Token 令牌机制（包括普通的 Access Token、自动更新的 Refresh Token，以及能有效解决跨认证的 JSON Web Token）等。在网页应用中，Session 经常被用于记录用户客户端的状态。与 Cookie 不同的是，它存放在网站的服务器上而不是存放在用户客户端的浏览器上。类比来说，在 Session 机制下，当用户第二次访问一家商店（网站）时，用户不再需要自己出示会员卡（Cookie）来证明自己的会员身份，而是由商店（网站）的工作人员通过自己内部的客户信息表（所存储的 Session）确认用户的会员身份。通过对客户信息表（多个 Session）属性的设置，每个用户只能获取和验证自己的会员身份，而不能对其他人的会员身份进行认证。

虽然从用户使用上更加方便，但 Session 增大了商店管理信息的压力（增加了服务器的压力）。因此，在很多大型网站，如 Google、Facebook、Twitter 等，都应用了可扩展性和安全性更好的 Token。Token 可以解决 Cookie 不可跨域性的问题，即能在两个域名之间跨过

域名来发送请求或获取数据，也更便于移动端使用，对内容分发网络（CDN）的支持性更好。

然而，这两项技术也有自身的应用缺陷。如 Session 机制在应用时会较多地消耗系统资源，在访问量较大时会影响网站的效率和稳定性。而且因为 Session 是基于 Cookie 进行用户识别，一旦 Cookie 被非法获取，基于 Session 机制的网站用户也容易遭受跨站请求的伪造攻击（简称为“CSRF “，是一种挟持用户在已登陆的 Web 应用上执行非用户本意操作的攻击方式）。而 Token 机制因其对加密特性的依赖，需要消耗比 Session 机制更多的系统资源。并且，和 Cookie 问题相似，Token 机制在使用过程中关于加密手段的安全性问题也须被重点关注。

此外，HTTP 协议提供的 ETag 实体标签，以及现代网站（包括 JavaScript 和 HTML5 其他编程语言）的语句中也都存在可以实现用于追踪的技术，如 Flash Cookie 伴随 Adobe 公司的 Flash（一个存储用户行为信息的解决方案）而出现，但 Flash 在多个浏览器已经被停用，Flash Cookie 已成为历史。

面对隐私问题时，以上这几项技术的机制目前还不够成熟，需要进一步的提升和改进。近几年，有一些新的概念和技术手段也频频被提出。新技术将实现相同的功能，并根据场景的特点和技术的特性不断完善，合理保护用户的隐私。相关原理与机制将在第七章第二节中具体分析。

四、对用户隐私挑战越来越甚，部分企业使用 Cookie 频繁被查

如前所述，为了满足广告主的精准化广告营销，第三方 Cookie 的产生能帮助实现这一目的。但由于其涉及用户个人数据传输给第三方的问题，一定意义上存在用户隐私方面的风险。比如，第三方 Cookie 会对用户广告观看等行为进行非常细致的记录，还可以记录用户在某一商品页面停留的时间和次数，观看某个特定广告的次数，而网站的运营者还可以通过 Cookie 控制单一用户对某一特定广告观看的次数。那么，这些个体的识别性数据会在没有任何技术手段控制后续使用的情况下，向数百个市场参与者予以披露，会严重损害到用户的隐私。因此，在全球隐私保护越来越严格的大环境下，很多国家或地区的数据保护机构已经向一些广告营销巨头展开调查，甚至通过直接处以巨额罚款进行惩戒。

（一）广告巨头 Criteo 被调查，Google 禁用第三方 Cookie

据美国一家专注于高科技和创业公司的媒体 TechCrunch 报道，为了回应国际隐私组织（Privacy International）于 2018 年 11 月提起的投诉，法国国家信息和自由委员会（the Commission Nationale de l'Informatique et des Libertés，以下简称“CNIL”）正在对广告科技巨

头 Criteo 展开基于 GDPR 的合规调查。[11]

国际隐私组织认为，Criteo 在线跟踪用户行为（包括但不仅限于 Cookie）不具有法律依据（Legal Basis）：既未征得用户的同意（User Consent），也不存在合法利益（Legitimate Interest）。尽管 Criteo 声称其收集处理用户数据的法律依据是因为存在合法利益，但国际隐私组织认为，合法利益要求进行平衡测试，以及考虑对个体利益的影响。虽然该案目前还未有新的进展，但如果 Criteo 真的违反 GDPR，CNIL 可对其处以最高达全球营业额 4%的罚款。

除 Criteo 使用 Cookie 被受问询以外，部分浏览器制造商采取了更为积极的行动来阻止第三方追踪技术的使用。据 TechCrunch 报道，2020 年 1 月 14 日，Google 宣布将在未来两年内禁止在 Chrome 中使用第三方 Cookie。[12]

（二）Google 与 Amazon 由于违规使用 Cookie 受到巨额处罚

2020 年 12 月 10 日，CNIL 宣布对于 Google（GOOGLE LLC 及 GOOGLE IRELAND LIMITED）和 Amazon（AMAZON EUROPE CORE）

[11] 参见 https://techcrunch.com/2020/03/10/adtech-giant-criteo-is-being-investigated-by-frances-data-watchdog/，最后访问日期 2021 年 2 月 18 日。

[12] 参见 https://techcrunch.com/2020/01/14/google-wants-to-phase-out-support-for-third-party-Cookies-in-chrome-within-two-years/，最后访问日期 2021 年 2 月 18 日。

公司违反法国数据保护法规定使用 Cookie 行为分别处以 1 亿欧元及 3500 万欧元的巨额罚款。

CNIL 认为，Google 的违规行为主要体现在以下三个方面：

（1）Google 在用户访问 google.fr 网站时，自动将用于广告营销用途的 Cookie 放置在其计算机中，但并没有要求用户对此做出同意；

（2）Google 并未以显著的方式，向访问 google.fr 网站的用户提供有关使用 Cookie 的信息；

（3）Google 向用户提供拒绝 Cookie 的机制（“opposition” mechanism）仅部分有效。[13]

对于 Amazon，CNIL 给出的具体处罚理由与 Google 的类似：

（1）当用户访问 amazon.fr 网站页面但尚未做任何操作前，Amazon 自动向其计算机中存入了大量用于广告营销目的的 Cookie，且未获得用户的同意；

（2）Amazon 向用户提供关于 Cookie 使用方面的信息不明确、不完整。[14]

[13] 参见 https://www.cnil.fr/en/Cookies-financial-penalties-60-million-euros-against-company-google-llc-and-40-million-euros-google-ireland，最后访问日期 2021 年 2 月 18 日。

[14] 参见 https://www.cnil.fr/fr/Cookies-sanction-de-35-millions-deuros-lencontre-damazon-

五、欧美法律体系下对 Cookie 的规制

（一）欧盟

如前所述，Cookie 为了实现其通信的必要性，会存储识别用户的个人数据，并且也会被用于追踪用户的行为，甚至被第三方读取，因此其存取的过程会对用户的个人隐私产生一定程度的侵扰。在欧盟，对 Cookie 的法律规制很早就有了，主要由《电子隐私指令》和 GDPR 等法律法规。除此以外，各成员国也分别制定了相关规则。下文将分别详细讨论各项具体的合规要求和实施条件。

1.《电子隐私指令》：同时满足告知和同意

欧盟 2002 年《电子隐私指令》（Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector）第 5（3）条规定，成员国应当确保，仅在根据《数据保护指令》（95/46/EC）向产品订阅者或用户告知了明确和全面的信息之后，才可以在订阅者或用户的终端设备中存储并访问所存储的信息。并且，成员国还应当同时向订阅者或

europe-core，最后访问日期 2021 年 2 月 18 日。

用户提供拒绝上述行为的权利。但这并不妨碍只是为了实现电子通信网络传输目的而进行任何技术存储或访问，或者为向用户提供服务之必须而实施上述行为。[15]

2009 年，欧盟对 2002 年《电子隐私指令》进行修订，修订后的《电子隐私指令》（Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws）第 2（5）条，则在 2002 年《电子隐私指令》的基础上补充，要求获得产品订阅者或用户的同意。[16]

[15] 2002/58/EC，Article 5（3）：Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/ 46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

[16] 2009/136/EC，Article 2（5）：Member States shall ensure that the storing of information,

由此可见，2002 年版的《电子隐私指令》只要求向用户告知并提供退出途径（Opt-out），而 2009 年版本的《电子隐私指令》，不但保留了 2002 年版《电子隐私指令》中的内容，还明确要求控制者向用户告知的同时，须取得用户的同意（Opt-in）。

同时，第 29 条工作组（Article 29 Working Party，以下简称“WP29”或“29 条工作组”）针对欧盟《电子隐私指令》中关于 Cookie 及类似技术发布过若干关键性指南。该类指南也尤其关注对用户同意的获取，包括《获取 Cookies 同意的指南》（Working Document 02/2013 providing guidance on obtaining consent for Cookies）及《Cookie 同意豁免意见》（Opinion 04/2012 on Cookie Consent Exemption）。

在《获取 Cookies 同意的指南》中，就获取用户同意问题提出了具体的、可操作性较强的实施指引。具体而言，该指南将获得用户对于 Cookie 使用的同意条件归纳为具体的信息、在先同意、主动和自由作出四项。

---

or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

（1）应当向用户提供具体的信息

首先，这要求网站运营者获取用户同意时告知的信息明确、易懂、可见。如将告知同意放置在进入页面首页，通常的做法是在浏览页面底部/顶部以横条或者悬浮窗的形式，向用户展示相关信息。网站还应当提供与所用 Cookie 相关的详细信息，并将通往该页面的链接以显著的方式呈现给用户。所提供的信息还应当包括不同 Cookie 各自的目的、保存期限等，并且应当告知用户对 Cookie 进行管理的方式（即如何接受全部或部分 Cookie 的使用，或拒绝使用 Cookie），而且需要标明第三方 Cookie 并对其进行说明。

（2）事前同意

网站运营者应当在向用户终端设备中存储 Cookie 前，事先获得用户的同意。不得在用户访问网站时就先向用户终端设备存入 Cookie，随后再进行告知或者不进行告知，即要求网站运营者对于 Cookie 的使用采取 Opt-in 的选择加入机制。

（3）积极主动作出同意

用户同意的行为应当是积极主动做出的，并且与其他常规浏览行为（如简单的滚动页面或了解详细信息）相区别。因此，网站应当单独向用户提供获取同意的机制(例如勾选选项框或者点击按钮),并且该机制

应当清楚、简洁、易于理解。当用户被充分告知了相关信息，并且主动做出选择的情况下，用户对于浏览器的设置可能被视为同意。但是，根据 WP29 在其相关意见(Working Party Opinion 2/2010)中的说明，通过设置浏览器代表同意的局限性非常强，一般难以适用。而法国《CNIL Cookie 指南》也指出，就现有技术而言，通过浏览器设置可能无法表示获取了用户的有效同意。

（4）自由作出同意

用户同意的行为应当是自由做出的。第一，应当在用户一打开页面，就可以看到关于 Cookie 的同意管理机制。该机制应当向用户提供精细化的 Cookie 同意选项（如分别征求用户对分析类、偏好类、营销类等不同类型 Cookie 的同意），同时应当确保用户随时都可以对做出的同意进行更改和撤回。这就意味着通过“Cookie 墙”（即 Cookie Wall，指数据控制者在网站中放置一个脚本，通过该脚本可以阻止用户访问网站的内容，如果用户不单击“接受 Cookie”的按钮，则无法访问网站的内容）的方式来强迫用户接受 Cookie 的行为是不符合要求的。

另，应当注意到，虽然 Cookie 的使用与个人数据的处理在很大程度上是互相重叠的，但是使用 Cookie 并不必然会涉及到对个人数据的处理。那么不涉及个人数据处理的 Cookie，在使用前是否也需要获取

用户的同意呢？对于这个问题，欧盟法院（以下简称“CJEU”）在 Planet49 案中已经做出了明确的回答，即《电子隐私指令》第 5（3）条的适用与 Cookie 是否构成 GDPR 定义的个人数据无关。[17]

修订后的《电子隐私指令》（2009/136/EC）第 5（3）条规定，“成员国应当确保，仅在根据《数据保护指令》（95/46/EC）向产品订阅者或用户告知了明确和全面的信息并取得其同意之后，才可以存储或访问在订阅者或用户终端设备中存储的信息，并且应当同时向订阅者或用户提供拒绝的权利。但这不妨碍只是为了实现电子通信网络传输目的而进行任何技术存储或访问，或者向用户提供服务所绝对必要的情况下使用。”其中提到在“只是为了实现电子通信网络传输的目的”及“向用户提供服务所绝对必要”两种情形下使用 Cookie 及类似技术无需提前获得用户同意。

WP29 在《Cookie 同意豁免意见》中，对于 Cookie 的分类，以及在何种情形下才可以豁免用户同意，结合一些具体应用场景，做出了更为详细的说明和解释，并认为满足以下情形的 Cookie 可以豁免用户同意：（1）用于记录用户输入内容的会话 Cookie（Session-id）或仅短期保留的 Cookie；（2）用于认证用途的会话 Cookie；（3）以用户为中心

[17] C-673/17 - Planet49, ECLI:EU:C:2019:801, para. 71.

的安全保护类 Cookie；（4）用于多媒体内容播放的会话 Cookie；（5）用于负载均衡的会话 Cookie；（6）保持 UI 个性化设置的会话 Cookie；（7）供已登录社交网络会员使用的第三方社交插件内容共享的 Cookie。

此外，虽然 WP29 在《Cookie 同意豁免意见》中指出，用于统计分析目的的 Cookie 属于非“严格必要”的 Cookie，即便是第一方 Cookie，也并不能满足豁免用户同意的条件。但是，WP29 同时也提到，如果网站在使用这类 Cookie 的时候提供了足够的保障措施、告知用户充足的相关信息、向用户提供易操作的选择退出机制、进行全面的匿名化操作，则使用这类 Cookie 给用户带来的隐私风险则极为有限。[18]

对于可豁免同意的“严格必要”的 Cookie 界定问题，一些成员国监管机构也对此做出了相应的说明，例如，《CNIL Cookie 指南》指出，根据法国《数据保护法》（1978 年 1 月 6 日第 78-17 号）第 82 条，符合下列条件的 Cookie 属于必要 Cookie，使用该类 Cookie 不需要将同意作为法律依据：（1）唯一的目的是实施在线交互；（2）根据用户明确要求且为用户提供在线服务所必须。[19]《ICO Cookie 指南》也指出，根

[18] Article 29 Working Party *Opinion 04/2012 on Cookie Consent Exemption,* at 11.

[19] CNIL *Guidelines relating to the application of article 82 of the law of January 6, 1978 modified to the operations of reading and writing in a user's terminal（especially Cookies and other tracers）*，Article 6：Article 82 provides that the requirement of prior consent does not apply if access to information stored in the user's terminal equipment or the recording of information in the user's terminal equipment:
- has the exclusive purpose of allowing or facilitating communication by electronic means; or

据 2003 年英国《隐私与电子通信条例》（Privacy and Electronic Communications Regulations，以下简称“PECR”）第 6（4）条，仅出于通过电子通信网络进行通信传输目的（也即所谓通信豁免，“communication exemption”），或者严格按照订阅者或用户要求提供信息社会服务所必要的 Cookie（也即所谓严格必要豁免，“strictly necessary exemption”），可豁免事先同意的要求。[20]

2.《电子隐私条例》（欧盟理事会通过版）：多项规制要求被提出

欧盟委员会于 2017 年 1 月 10 日发布了《电子隐私条例》（E-Privacy Regulation，以下简称“E-PR”）的提案。经多轮讨论和修改，欧盟理事会于 2021 年 2 月 10 日发布了欧盟理事会定稿版，目前欧盟理事会和欧盟议会正在进行正式发布前的最终协商。E-PR 在《电子隐私指令》的基础上扩大了规制对象的范围，即将规则要求涵盖所有的电子通讯服务提供商，例如 WhatsApp、Facebook

- is strictly necessary for the provision of an online communication service at the express request of the user.

[20] ICO *Guidance on the use of Cookies and similar technologies*：Are we required to provide information and obtain consent for all Cookies? No – PECR has two exemptions to the Cookie rules. Regulation 6(4) states that:

(4) Paragraph (1) shall not apply to the technical storage of, or access to, information -

(a) for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or

(b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.

Messenger、Skype、Gmail、iMessage 等，并且，对于利用 Cookie 等同类技术在线追踪用户个人信息中产生的问题作出了重要的规定，不但赋予了用户知情权，还要求网络运营者征得用户同意，同时也赋予了用户以一定程度的自主控制权。具体规定如下：

（1）必须通过 Banner 申请 Cookie 同意的需求被删除；E-PR 指出，目前，追踪类 Cookie 及同类在线追踪技术被广泛使用，频繁的同意请求可能导致用户不愿查看与请求相关的信息，从而导致个人信息保护水平的下降，所以允许通过软件设置授权同意的方法来解决前述问题，比如添加授权同意使用特定类型 Cookie 的服务商白名单；

（2）不侵犯用户隐私或对于隐私的侵害性非常小的 Cookie，则无需征得用户的同意，例如交易场景下使用验证用户身份的 Cookie、使用 Cookie 以保存用户放置购物车中物品记录等；除此之外，E-PR 认为在评估已交付的信息服务（例如网站设计和广告）的有效性时，或在统计访问网站的终端用户数量、网站的特定页面或应用程序的终端用户数量时，Cookie 是有效且合法工作的。但是，如果 Cookie 和其他类似标识符的使用是用于确定使用该网站的具体个人，则需要终端用户的同意。

（3）终端用户授权同意某网站存储 Cookie 或类似标识符，也意味着在用户再次访问该网站时，网站无需再次授权即可读取 Cookie。

（4） 原则上禁止使用 Cookie 墙（“Cookie 墙”的具体解释请见下节），但如果为用户提供了不涉及需要对 Cookie 和其他同类追踪技术表示同意的选项，则可允许。某些情况下，如果终端用户和服务提供商之间存在明显的失衡（比如该网站用于实现由特定政府机关提供的服务，或服务提供商处于市场主导地位的），且访问该类网页必须同意 Cookie 才能使用，则会被认为剥夺了用户真正的选择权。

3.《通用数据保护条例》：同意标准需要合规

2018 年正式实施的 GDPR 将“个人数据”定义为可以被用来直接或间接识别自然人的任何信息。若 Cookie 中存储的数据可以单独或与其他信息结合识别特定自然人的，则需要同时受到 GDPR 的规制。

GDPR 列出了六项处理个人数据的法律依据，包括用户同意、合法利益等。根据 GDPR 第 4（11）条，“同意”指的是数据主体通过声明或明确而肯定的动作（clear affirmative action）、自由作出的（freely given）、具体的（specific）、知情的（informed）、明确的（unambiguous）表明同意对其相关个人数据进行处理的意愿。[21]

根据 GDPR 第 7 条，当个人数据的处理是建立在同意的基础上，

[21] GDPR，Article 4（11）：”consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

数据控制者需要能够证明数据主体已经作出同意；如果数据主体的同意是在涉及有关其他事项书面声明的情形下作出的，征得用户同意的请求应当完全区别于其他事项，以一种普通人容易理解的形式，使用清晰和平白的语言进行表达；并且，应当确保数据主体有权随时撤回其同意，撤回同意的方式应当和作出同意一样简便；对于判断同意是否满足“自由作出”这一要件，如果同意并非合同履行所必要，但合同的履行（如提供服务）取决于同意，该同意则推定为不是基于自由意志做出的。[22]

CJEU 于 2019 年 10 月 1 日对 Planet 49 案做出了判决（案例细节参见下述第 5 点）。在该案中，CJEU 分析了使用 Cookie 和类似技术的透明度和同意的标准。CJEU 在判决中指出，不论 Cookie 数据是否构成个人数据，《电子隐私指令》第 5（3）条对使用 Cookie 的同意规则均要参照适用 GDPR 的同意标准。[23]

2020 年 5 月 4 日，欧洲数据保护委员会（以下简称“EDPB”）通过了《对第 2016/679 号条例（GDPR）下同意指南 v1.1》[24]（以下简

[22] GDPR，Recital 43.

[23] Lennart Schüßler, James Fenelon, *Planet49: CJEU Rules on Cookie Consent*, 参见 https://www.twobirds.com/en/news/articles/2019/global/planet49-cjeu-rules-on-Cookie-consent，最后访问日期 2021 年 2 月 18 日。

[24] EDPB *Guidelines 05/2020 on consent under Regulation 2016/679.*

称“《EDPB 同意指南》”），对 GDPR 的同意标准做出了细致的说明。这也是对第 29 条工作组于 2018 年 4 月通过的《WP29 对第 2016/679 号条例下同意指南》的更新版本，主要对如下两个问题进行了进一步澄清：

（1）关于数据主体在与所谓的“Cookie 墙”进行交互时，所提供同意的有效性；

（2）数据主体“滚动页面”的操作行为是否构成“有效”同意。

《EDPB 同意指南》明确指出，“Cookie 墙”违反 GDPR 下数据主体作出同意时的“自由”要件。因为“Cookie 墙”将网络运营者向订阅用户或用户终端设备中存储信息并进行访问的行为作为用户使用其网站服务和功能的前提条件，不构成向用户提供真正的选择，故《EDPB 同意指南》明确表示，通过“Cookie 墙”所获得的用户同意不视为有效同意。[25]

此外，GDPR 中规定的有效同意需要数据主体“明确表达意愿”，即需要数据主体作出声明或明确且肯定的行为，该行为必须是明显无疑的。这要求数据主体必须采取积极的行动来表明同意特定的数据处理行为，也要求控制者确保能够将数据主体作出同意的动作与其他动

[25] EDPB *Guidelines 05/2020 on consent under Regulation 2016/679*，para.39-41.

作相区分。因此，单纯地继续常规性使用网站服务的行为（即“滚动”或“滑动”页面等操作）不足以被推定为数据主体同意网站所声明的数据处理操作；该行为由于很难与用户在网站上的普通操作或交互行为相区别，不是明确的同意行为。因此，《EDPB 同意指南》明确，数据主体滚动页面操作的行为亦不构成有效的同意。[26] 故，对于必须征得用户同意才能开启的 Cookie，如果用户仅仅滚动页面并未点击同意 Cookie 按钮，则不得开启该等 Cookie；只有用户明确点击“同意”，方可开启。

4. 欧盟各国及英国监管机构对 Cookie 及类似追踪技术的指南

欧盟除了有以上介绍的对欧盟各成员国普遍适用的法规与指南外，各成员国国内监管机构针对 Cookie 技术也发布了不同的指南，结合本地要求进行规定。

2019 年 3 月，德国监管机构会议（the German Conference of Supervisory Authorities 以下简称“GDPA”）发布了《有关在线跟踪技术的指南》（Guidance on internet tracking）。

2019 年 7 月，法国 CNIL 发布了关于 Cookie 及类似技术适用《法国数据保护法案》（the French Data Protection Act）第 82 条的

[26] EDPB *Guidelines 05/2020 on consent under Regulation 2016/679*，para.84-86.

指南（Guidelines relating to the application of article 82 of the law of January 6, 1978 modified to the operations of reading and writing in a user's terminal（especially Cookies and other tracers），以下简称“《CNIL Cookie 指南》”）并于 2020 年 9 月更新。2020 年 1 月，CNIL 还发布了《关于使用 Cookie 和其他追踪技术的建议（草案）》（Draft recommendation on Cookies and other trackers），并于 2020 年 9 月正式发布定稿版本（以下简称“《CNIL Cookie 建议》”）。《CNIL Cookie 建议》旨在从实际操作的层面向企业提供合规建议。

2020 年 2 月，希腊数据保护局（Hellenic Data Protection Authority，以下简称“HDPA”）针对互联网 Cookies 和追踪器发布使用指南（Guidelines on the use of internet Cookies and trackers，以下简称“《HDPA Cookie 指南》”）。

英国监管机构同样就 Cookie 的问题发布专门指南。2019 年 7 月，英国信息专员办公室（Information Commissioner's Office，以下简称“ICO”）发布了《关于使用 Cookie 及类似技术的指南》（Guidance on the use of Cookies and similar technologies 以下简称 “《ICO Cookie 指南》”），主要围绕如何提供有关 Cookie“明确和全面的信息”以及“如何获取用户的有效同意”的实践指引。

我们通过对上述提及的欧盟各国及英国监管机构分别发布的对 Cookie 的指南进行对比分析，发现这些监管机构的观点既存在共性，也存在不同之处。

其中，共性大致有以下六点：

（1）指南是否仅适用于 Cookie 技术：四国数据保护机构都认为指南中的规则不仅适用于 Cookie 这一种技术，适用于在用户设备上存储或访问个人信息的任何其他技术（移动应用程序中的软件开发套件、本地对象、浏览器指纹技术等）。

（2）默认同意无效：四个国家的数据保护机构都认为如果需要征得用户的同意，则网络服务提供者必须在用户数据收集开始之前由用户给予特定的、自愿的和明确的同意。用户继续浏览网站等行为并不代表该用户作出了同意的表示。

（3）用户明确同意的对象和细节：法国 CNIL 和英国 ICO 都表示，发布网站的条款和条件（Terms and Conditions）不能用作获取同意的方法。根据 GDPR 第 7 条第 2 款的规定，网络服务提供者需要获取用户明确的、特定的、针对数据处理的同意。

（4）Cookie 的使用目的：网络服务提供者必须告知用户收集和处理其数据的所有目的，即所有使用 Cookie 的目的。CNIL 还要求网络服

务提供者获取分别针对每个数据使用目的的、特定的同意。虽然《ICO Cookie 指南》中未对此进行详细说明，但根据 ICO 的自身实践，他们有较大可能性也会这么做。GDPA 的指南要求获得详细、明确的用户同意，但没有详细说明分层关系。HDPA 在其指南中还明确指出数据控制者应当告知所使用的每一个追踪技术的目的，不应提供笼统的目的描述。

（5）浏览器设置：四国数据保护机构都指出，仅仅通过浏览器设置允许 Cookie 的使用不视为获得有效的同意。

（6）涉及到的关联方列表：四国数据保护机构都规定，用户必须能够识别所有处理其数据的关联方。

当然，四国数据保护机构对于 Cookie 的规制也存在细微的差别，主要从以下五个维度梳理：

对比维度	法国	英国	德国	希腊
是否可以使用没有“拒绝”选项的 Cookie 弹窗？	**不能**，剥夺用户拒绝 Cookie 收集数据的权利可能会带来严重的后果。	通过这样的 Cookie 弹窗强制执行的同意“**不太可能有效**”。但是，GDPR 也必须与其他权利（包括言论自由和开展业务的自由）保持平衡。	同法国，**不能剥夺拒绝的权利。**	同法国与德国，**不能。**
分析类 Cookie	**不总是。**如果某些分析性	**必须获得同意，没有例外。**尽管 ICO	**不需要**获得同意，除非使用该	**大概率需要获得同意。**用于

（Analytic Cookie）是否需要获取同意？	Cookie 满足 CNIL 提供的一系列要求，则可以免除事先同意。	指出“在侵入性程度较低且对个人造成伤害的风险较低的情况下，使用 Cookie 采取任何正式行动的可能性不大”，并且以分析性 Cookie 为例，证明了其较低的风险，但仍然规定必须获取事先同意。	Cookie 会导致将个人数据转移给第三方。即使在那种情况下，如果用户可以轻松选择退出向第三方传输数据，则无需征得用户的事先同意。	广告营销目的的追踪技术需要获得用户的知情同意。尽管《HDPA Cookie 指南》中指出了豁免同意的情形，但一般不涉及分析类 Cookie。
同意是否作为后续处理个人数据的基础？	用户同意并**不是**后续进行个人数据处理的**唯一**法律基础。	处理与 Cookie 相关的数据，大多数情况下，用户的**事先同意应当作为其法律依据，而不是依靠合法权益。**处理与个人信息相关的数据，合法权益永远不能作为法律依据。	和法国类似，德国**不认为**用户的事先同意总是必须的。	同法国，用户同意并**不是**后续进行个人数据处理的**唯一**法律基础。
如何为用户提供的“同意”和“拒绝”的设置选项？	同意必须是用户主动且明确作出的，**如果用户未明确作出同意的选项，则视为用户拒绝 Cookie 的使用。** 同时，建议在用户可浏览的每一页都设置“Cookie”	不得在 Cookie 选项上强调“同意”或“允许”，这种强调会影响用户选择“接受”。 不得将“拒绝”或“阻止”选项放置于第二层，而“同意”/“允许”Cookie 选项位放置于第一层。	带有 Cookie 信息和一个简单的“确定”按钮是不够的，用户的同意必须是可识别的。即，Cookie 弹窗**必须详细列出**所有需要同意的数据处理活动，并且用户必须**能够拒绝**这些选项。但未针对每个数据处理活动的具体选项明确是否可	应提供给用户同样**简洁、易操**作的同意和拒绝选项。 同时，为了避免用户的自由选择受到影响，推荐将同意和拒绝的选项设计为**同样的字体大小与颜色。**

	键,以便用户随时撤回同意。		以分层设计（例如提供一个“接受全部”选项）。	
Cookie 的操作和保留期限	强调保存用户同意或拒绝记录的重要性,并推荐**保存 6 个月**的最佳实践。（注:旧版指南中要求最多保存13个月的要求在最新的指南中被删除。）	Cookie 的保留期限必须**与预期结果成比例**,仅限于达到目的所需要的期限。Cookie 的理论性最长操作周期（例如“31/12/9999”）在任何情况下均不视为相称。	没有具体制定。但德国认为**较短的操作周期**（也称为“可识别期”）更可能更满足GDPR利益平衡测试的要求(GDPR6(1)(f))。	未进行明确。

我们初步理解，GDPR 对于使用 Cookie 技术的态度是网络服务提供者应当保障用户知情权，原则上使用 Cookie 需要提前征得用户的同意,要遵守 GDPR 关于个人信息保护的一般原则。虽然欧盟国家和英国对 Cookie 的规制要求有很多相似性,但在具体细节上还是有不少差异，因此，企业在实务中还应当参考各国的具体规定、案例以及指南。本报告附表针对英国、法国、德国及希腊的《Cookie 指南》进行了更为详细的介绍和横向比对梳理，希望有助于读者进行更加深入和具体的理解。

此外,丹麦数据保护局（Datatilsynet）于 2021 年 2 月 12 日与丹麦数字安全委员会和丹麦商业局一起发布了有关 Cookie 使用的快速指南。主要包括以下几点：

1. 设置 Cookie 之前必须征得同意；

2. 必须采取积极行动才能被视为有效同意；

3. 必须为用户提供接受和拒绝使用 Cookie 的平等机会；

4. 在获得用户同意之前，只能设置使用必要型的 Cookie；

5. 用户的同意必须记录在案；

6. 户必须能够轻松地撤回其同意；

7. 用必须有关于 Cookie 的目的和有效期的明确信息；并且

8. Cookies 声明/隐私声明中应说明用于后续处理个人数据的任何其他法律依据。

因此 ,最新丹麦 Cookie 指南 ,基本和其他欧盟国家思路如出一辙。

5. 标志案—德国 Planet49 网站使用 Cookie 案等

德国“Planet49”公司在其网站上举行了一次促销抽奖活动。参与抽奖活动的用户在注册时，Planet49 要求其同意：（1）Planet49 可以使用跟踪用户线上行为的 Cookie；以及（2）接受第三方的广告信息。为了达成上述两个事项，企图通过 Cookie 收集用户信息从而达到宣传

Planet49 合作伙伴产品的目的。为此，Planet49 使用了获取 Cookie 同意的“复选框”形式，并对该复选框进行了预先勾选。

德国消费者组织联合会声称，这两个复选框不符合德国法律的要求，并向法院寻求强制令，要求 Planet49 停止使用复选框。该案最终提交至德国联邦法院（以下简称“FCJ”），后来 FCJ 又将该案转交给 CJEU 就欧盟有关保护电子通信隐私法律（informed consent）的适用进行解释。

（1） CJEU 认定德国 Planet 49 公司使用 Cookie 追踪用户信息不合规[27]

CJEU 经过审查认为：授权同意使用 Cookie 和类似技术的预选复选框不构成《电子隐私指令》下的有效同意；《电子隐私指令》第 5 条第 3 款的 **Cookie 同意规则，适用 GDPR 的同意标准，且不论 Cookie 数据是否构成个人数据**；网站运营者必须向网站用户提供有关 Cookie 持续时间以及第三方是否可以访问 Cookie 的相关信息。具体而言，CJEU 的判决要点如下：

- 预先选中的复选框不构成有效同意

[27]参见 http://curia.europa.eu/juris/document/document.jsf?text=Cookie&docid=212023&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=3758434#ctx1，最后访问日期 2021 年 2 月 18 日。

CJEU 指出，预先选中的复选框不构成使用 Cookie 或类似技术的有效同意。

首先，《电子隐私指令》明确要求网络服务提供者在用户终端设备中存储并访问信息的行为需要事先征得用户的同意。但是，《电子隐私指令》并未指明同意所须采用的形式。CJEU 针对“得到他/她的同意”一词进行了字面解释，认为使用者必须“表明”其意愿。这意味着，用户必须执行一项主动的操作，而非被动的接受。**网站用户必须对其设备上 Cookie 的存储和访问具有足够的控制力。**

根据 CJEU，以预选复选框的形式表示同意并不构成主动的行为。通过不取消预先选中的复选框来客观地确定用户是否已给出了知情同意“似乎是不可能的”。并且，用户在继续访问目标网站之前也可能没有看到或阅读到该复选框。

此外，GDPR 明确要求积极、具体的同意，并禁止将“沉默”、“预先勾选”或“无所作为”构成同意。在这种背景下，**Planet 49 网站采取“预先勾选”复选框征得用户对于存储 Cookies 的同意是无效的。**

● Cookie 收集非个人数据也需用户同意

毫无疑问，Planet 49 将姓名、地址与用户参与促销抽奖活动的注册账号相关联，因此其收集的 Cookie 数据是个人数据。

CJEU 对大多数从业者明晰的要求进行了确认，即无论是否处理个人数据，《电子隐私指令》中关于 Cookie 的同意规则均适用。在这一点上，CJEU 同意了总检察长的意见，认为《电子隐私指令》的立法目的是为了防止干扰用户的“私有领域”。该“私有领域”包括存储在用户设备上的任何信息，因此无论存储或访问的信息是否为个人信息，《电子隐私指令》都将用以“保护用户免受隐藏标识符在他们不知情的情况下进入他们设备的风险”，且《电子隐私指令》第 5 条第 3 款关于 Cookie 的同意适用于 GDPR 的同意标准。

● 透明度：存储时间和第三方访问权限

在透明度方面，网站运营商必须告知用户 Cookie 的存储时间以及第三方的访问权限。CJEU 认为，提供有关 Cookie 存储时间的信息是基于公平处理原则的要求。将 Cookie 信息保留很长时间甚至无限期保留，意味着收集了用户大量有关浏览历史记录的数据，且违反了公平处理甚至存储限制原则。因此，网站运营者需要提供有关 Cookie 数据存储期限的信息，以便用户可以确定是否同意在其设备上开启 Cookie 以及知悉相关后果。CJEU 还指出，如果无法做到明确各类数据的存储期限，根据 GDPR 第 13 条，控制者应至少向用户告知确定存储期限的标准。

同样，基于 GDPR 第 13 条关于要求数据控制者提供数据接收方名称或类别，CJEU 还指出，网站运营商必须告知用户有权访问 Cookie 的

第三方：只有在提供数据实际接收者信息的情况下，用户做出的同意才会被认为是“知情”的。

● 激励同意

Planet49 将用户同意其个人数据用于广告目的作为用户参与促销抽奖活动的前提条件，这或可被视为一种激励用户给予同意的机制。但目前，FCJ 没有请求 CJEU 就这一条件是否符合 GDPR 下“自由给予”的标准进行说明。

（2） 德国联邦法院：“ Cookie Consent II”裁定

根据 CJEU 的判决，FCJ 于 2020 年 5 月 29 日对 Planet 49 案做出如下裁定（文件编号：I ZR 7/16，以下简称“Cookie Consent II”裁定）：

● 必须根据《电子隐私指令》解释《德国电信媒体法案》（以下简称“TMG”）第 15 条第 3 款（该条款为使用 Cookie 提供了法定依据）；

● 使用 Cookie 进行营销或用于市场研究需要用户同意；

● 无论 Cookie 是否收集个人数据，Cookie 的有效同意要件均适用；

● 必须通过用户积极的确认给予同意。预先选中复选框既无法满足

TMG 的要求，也不能符合 GDPR 的要求；

● 为了满足“知情同意”的要求，运营者提供的信息必须详细，但不能过多，因为大量信息会妨碍用户有效地理解被提供的信息。

在 Cookie Consent II 裁定中，FCJ 进一步澄清了知情同意的要求。Planet49 曾试图促使用户同意 Planet49 赞助商和合作伙伴能够通过电话、短信、邮件或电子邮件的方式向用户发送市场营销信息。为了获取用户的此项同意，Planet49 并未使用预先选中的复选框，而是向用户提供了链接到 57 家第三方赞助商和合作伙伴公司列表的通用同意文本，要求参与者逐个决定是否接收被链接公司的营销信息。如果没有选择，Planet49 将代表参与者做出决定。

FCJ 认为，虽然没有预先勾选复选框，但此设置也不构成知情同意。知情同意要求：（1）参与者知道他们所同意的内容；以及（2）他们的同意涵盖了所涉及的产品和服务。向用户提供过多的选择，实际上无法满足上述要求。过多的选择只会导致用户不愿查看“簇堆”的信息和有耐心地做出自由的决定。并且，在用户未能做出决定的情况下，Planet49 也不能自动代表用户做出决定。法院最终裁定，用户的同意并非主动给出的，也不是知情状态下给出的，因为用户面对被提供的大量选择而不知所措，从而无法适当注意应当获得的信息。

长期以来，一直存在一个关于 TMG 是否执行《电子隐私指令》的

问题。FCJ 的上述裁定明确表示，需要根据《电子隐私指令》对 TMG 的相关条款进行解释和适用。在此之前，德国联邦经济事务和能源部已经宣布，在不久将进行的对 TMG 的修订中，考虑 CJEU 对 Planet49 案的判决。此外，CJEU 的判决也非常符合德国数据保护机构先前发布的指南要求。

（3） 英国法院判定谷歌擅自将 Cookie 植入浏览器收集用户信息违法[28]

2015 年，三名英国公民起诉谷歌公司，诉称谷歌公司通过向苹果公司 Safari 浏览器中植入 DoubleClick ID Cookie 的方式，在未向用户告知、未征得用户同意的情况下，采集用户使用 Safari 浏览器时产生的数据（Browser Generated Information），例如，上网记录、上网习惯、社会地位、种族与民族、性取向、经纪状况、精神与身体健康情况等个人信息。谷歌公司采集用户的个人信息后，对用户进行了个体画像，并通过向用户推送个性化广告的方式进行盈利。尽管 Safari 网页浏览器默认的隐私设置允许用户从跟踪用户的第三方 Cookie 中退出，但是尽管如此，用户的个人信息仍会通过“Safariworkaround”被搜集。在特定时期内，由于在用户尚未知晓或同意的情况下运行

[28] 参见 https://www.supremecourt.uk/news/permission-to-appeal-decisions-28-july-2015.html，最后访问日期 2021 年 2 月 18 日。

Safariworkaround，谷歌公司由此获得并记录了上述个人信息。谷歌在上诉法院的判决中败诉，寻求向英国最高法院进行上诉。

类似的事件还有，2018 年，英国苹果手机用户组成了“Google You Owe Us”的组织，意图向谷歌公司发起集体诉讼，要求谷歌公司就其绕开苹果公司防止第三方 Cookie 跟踪用户的机制，在未征得用户同意的情形下收集个人信息用于个性化展示进行巨额赔偿。

（4） 比利时隐私保护委员会认定 Facebook 通过 Cookie 处理非注册用户的浏览器数据违法[29]

Facebook 提供了一款社交插件，网站所有者可以将这款插件放置在他们的网站中，以使网站访问者作出一定的行为，例如“喜欢”该网站的内容，对其做出反应或进行分享等。当互联网用户向包含社交插件的网站作出一定请求时，浏览器会将该请求发送到 Facebook 服务器，此时发送至 Facebook 服务器的内容包括用户 IP 地址、网站的 URL、操作系统浏览器的类型，以及先前由 Facebook 服务器放置在浏览器的 Cookie 等。

无论用户是否为注册用户，Facebook 将包含唯一浏览器标识符的

[29] 参见 https://edps.europa.eu/sites/edp/files/publication/16-03-15_case_law_overview_2015_en.pdf，最后访问日期 2021 年 2 月 18 日。

Cookie（“datr Cookie”）放置在任何访问 facebook.com 域网站用户的浏览器中。该 Cookie 会在用户的计算机上保留 2 年。Facebook Ireland 公司保留包含匿名 datr Cookie 标识符和 IP 详细地址的访问日志。通过此种方式，Facebook 可以综合 datr Cookie、IP 地址和用户访问的网站来监视互联网用户的上网行为。

比利时隐私保护机构发布了一项建议，强调通过 Cookie 和社交插件获得个人信息、对有关未注册用户的数据进行处理不符合比利时隐私立法，并责令 Facebook 避免在系统中放置记录非注册用户个人信息的长时间和唯一标识符 Cookie。由于 Facebook 公司未能遵守该命令，比利时隐私委员会后来向 Facebook 公司提起诉讼，要求 Facebook 停止（1）向未经注册的用户浏览器放置 datr Cookie；以及（2）通过社交插件收集第三方网站上的 Cookie 信息。

法院认为，征得个人信息主体的同意需要个人信息主体在清晰、明了地了解收集其个人信息的情况后，给出明确的同意。当互联网用户首次访问 facebook.com 网站时，Facebook 会显示 Cookie Banner，警告其使用 Cookie 并提供指向 Cookie 声明的链接。如果用户单击 Cookie 声明页面上的超链接（例如“Facebook 服务”），则将开启 datr Cookie。法院认为，这并不构成知情同意，因为用户仍然处于了解通过 Cookie 哪些信息被收集，而非表达同意的阶段。

2015 年，法院最终判令 Facebook Inc、Facebook Belgium Sprl 和 Facebook Ireland Limited 停止针对非注册用户的行为：（1）在未向用户充分、适当地告知 Facebook 放置 datr Cookie 的事实以及 Facebook 将如何使用该 datr Cookie 方式的情况下，在所属 facebook.com 域名的网页上放置 datr Cookie；（2）通过在第三方网站上放置社交插件收集 datr Cookie。此外，法院还对不遵守该命令处以每天 25 万欧元的罚款。

（5）CNIL 对谷歌 Cookie 违法使用开出一亿欧元天价罚单[30]

CNIL 于 2020 年 3 月 16 日对 google.fr 网站进行了调查，发现用户登录到该网站后，即便不进行任何操作，也会有七个 Cookies 被自动置入其终端设备中。谷歌爱尔兰公司在 2020 年 4 月 30 日的回应信函中表示，七个 Cookies 中有四个 Cookies 意在进行广告推广。CNIL 认为，谷歌的行为主要从三方面违反了《法国数据保护法》第 82 条的规定。

首先，谷歌未向用户提供足够清楚明确的信息。本案调查中发现当用户进入 google.fr 页面时，底部会显示一个 Banner（横条），其中包含关于谷歌隐私政策的提示信息，另一侧有两个按钮，分别为“稍后提

[30] 参见 https://www.cnil.fr/en/cookies-financial-penalties-60-million-euros-against-company-google-llc-and-40-million-euros-google-ireland，最后访问日期 2021 年 2 月 27 日。

醒我”和“立即查看”，但并未向用户告知会在终端设备上储存 Cookie 的信息。当点击“立即查看”时，弹窗内容中尚未包含任何关于 Cookie 和其他追踪技术的使用信息，同时该弹窗所展示的隐私政策中也没有明确提及适用于 Cookie 的规则。

其次，谷歌未获得用户同意即使用 Cookie。如本案例开头提到，当用户登录到 google.fr 网站后，在未经用户同意的情况下，七个 Cookies 会被自动存入用户的终端设备中，且其中有四个用于广告营销用途。

最后，调查发现谷歌向用户提供的禁用 Cookie 机制部分无效。用户在点击 google.fr 页面下方信息栏处的“立即查看”后，页面会跳出窗口，用户可点击窗口中的更改广告设置按钮，然后可通过滑动按钮来禁用谷歌搜索广告个性化和网页广告个性化。一旦用户拖动此滑动按钮关闭个性化广告后，页面会跳出新的窗口，要求用户确认自己的选择，并告知关闭的仅是个性化广告功能但不会影响普通广告的投放。然而，当用户选择关闭个性化广告后，尽管浏览器通过选择退出值，向与其链接的服务器表明用户已表示拒绝接受今后从该域存入相同的 Cookie，实际上，当用户继续浏览网页时，仍会有多条广告 Cookie 继续储存到该用户的终端设备上。当 Cookie 域重新与相关域交互时，含 Cookie 域的服务器（例如，google.com 或 google.fr）可以重新读取 Cookie 中所包含的信息。

基于上述事实，CNIL 于 2020 年 12 月 10 日对谷歌公司及谷歌爱尔兰公司处以共计 1 亿欧元的天价罚单，并要求谷歌公司及谷歌爱尔兰公司在三个月内完成在 google.fr 网站首页的 Cookie Banner 中告知用户 Cookie 的用途以及用户的拒绝方式，若逾期则处每日 10 万欧元的滞纳金。

6. 小结

总体而言，欧盟各成员国发布的有关使用 Cookie 的指南均强调，除为提供通信传输或用户所要求的在线服务必须的情形外，所使用的 Cookie，也即所谓非必要 Cookie，需以用户同意为法律依据，在征得用户同意方面适用 GDPR 关于用户同意的标准。同时注意在《电子隐私条例》未正式生效前，各国仍可能存在规定不一致、执法不一致的情况。欧盟处罚案例则进一步召示了监管执法趋势。

（二）美国

与欧盟不同的是，美国没有专门针对 Cookie 的法案。在联邦层面，主要包括《电子通信隐私法》（the Electronic Communications Privacy Act，以下简称“ECPA”）、《联邦窃听法》（Federal Wiretap Act，以下简称“FWA”）、《计算机欺诈和滥用法》（the Computer Fraud and Abuse Act，以下简称“CFAA”）。根据 ECPA（18 U.S. Code § 2701），

任何擅自故意使用电子通信服务设施或故意超过授权范围进入该设施并获取、改变或阻止通信授权访问的行为，将受到惩罚，除非该行为经过授权或满足法律规定的其他例外情形。FWA（18 U.S. Code § 2511）禁止窃听和泄露电线、口头或电子通讯，除非获得一方或者双方的同意。CFAA（18 U.S.C. § 1030）禁止未经授权故意进入受保护的电脑以获取资讯，但需要单次行为至少造成 5000 美元的损失。

此外，联邦层面还针对特殊行业或人群的个人信息进行规制，例如健康医疗领域的《健康保险可携与责任法》（Health Insurance Portability and Accountability Act）、金融领域的《格雷姆-里奇-比利雷法案》(Gramm-Leach-Bliley Act)、针对儿童的《儿童在线隐私保护法》（Children's Online Privacy Protection Act，以下简称"COPPA"）。其中，COPPA 下的个人信息包括持久性标识（persistent identifier），包括但不限于 Cookie 中保存的用户编号、IP 地址、设备序列号或唯一设备标识符等（§312.2）。据此，适用 COPPA 的企业需要获得监护人可验证的同意（verifiable parental consent）。

在州法层面，加州在个人信息和隐私保护方面的立法较为领先。《加州在线隐私保护法案》（California Online Privacy Protection Act of 2003，以下简称"CalOPPA"）要求商业网站和在线服务的运营商制定隐私政策，披露他们如何收集个人信息，其中包括与其他信息一起以"个

人识别形式”存储下来的网站或在线服务收集的信息（例如 Cookie）。根据 CalOPPA，企业的隐私政策应当包括浏览器对“Do Not Track”相关机制的回应方式（§22575）。

《加州消费者隐私法案》（California Consumer Privacy Act of 2018 ）（以下简称“CCPA”）及加州总检察长办公室颁布的《加州消费者隐私法条例》（California Consumer Privacy Act Regulations）（以下简称“CPRA”）将 Cookie 作为一种在线标识符（“Unique Identifier”或“Unique Personal Identifier”）明确纳入个人信息范畴内（§1798.140）。CCPA 要求企业在收集时或之前向消费者告知收集和处理个人信息类别，并赋予加州居民相关权利，包括知情权（Right to Know）、删除权（Right to Delete）、更正权（Right to Correct）、退出权（Right to Opt-out）等。其中，就退出权而言，企业尤其需要注意向消费者提供可以由消费者拒绝将 Cookie 相关数据出售给第三方的选择。同时，如果该第三方在公司网站上放置 Cookie，双方必须签订保护消费者信息的合同条款。

在 Doubleclick INC. Privacy Litigation 案中，用户起诉 Doubleclick，称 Doubleclick 在用户的电脑硬盘驱动器上放置 Web Cookie 的行为违反 ECPA、FWA 和 CFAA。在该案中，当用户访问 Doubleclick 网站时，Doubleclick 会在每个用户的电脑硬盘上放置一

个 Cookie。DoubleClick 的服务器通过 Cookie 标识号识别用户的配置文件，利用 Cookie 跟踪用户的网络活动，并建立用户档案，以提供有针对性的广告。原告诉称，Doubleclick 获取 Web Cookie 中用户信息的行为构成未经授权的访问，同时构成窃听用户与其他网站的通信。

法院认为，Doubleclick 的行为属于 ECPA 和 FWA 规定的同意例外（Consent Exception）。此外，其行为虽然违反 CFAA，但由于对用户计算机上 Cookie 的每次访问都构成一个单独的未授权访问行为，因此损害和损失只能针对每个 Cookie，而不能计算多个计算机的损失之和。因为单个 Cookie 造成的损害未达到 5,000 美元的法定损失门槛，因此 Doubleclick 无需承担责任。据此，法院判决 Doubleclick 不承担责任。

Google 除在欧盟面临相关处罚外，在美国，也曾因被指绕过 Safari 和 Internet Explorer 的隐私设置，跟踪互联网用户信息，因而面临多家组织的集体诉讼。2017 年 2 月，美国特拉华州地区法官苏·罗宾逊（Sue Robinson）批准了和解协议，根据和解协议，Google 将停止在 Safari 浏览器上使用 Cookie，并将 550 万美元支付给原告。该和解协议于 2019 年 8 月 6 日被美国联邦第三巡回上诉法院予以驳回，称无法判定 550 万美元的和解是否公平、合理和充分，并表示下级法院法官应重新审理此案。

总体而言，除儿童这类特殊群体需要 Opt-in 以外，美国对于 Cookie 的规制采用 Opt-out 机制，整体侧重于要求企业进行完整披露并进行有效响应。

六、我国法律体系下对 Cookie 的规制

（一）相关法律法规及国家标准下的 Cookie 规制要求

根据《中华人民共和国网络安全法》（以下简称“《网络安全法》”）第四十一条和《中华人民共和国民法典》（以下简称“《民法典》”）第一千零三十五条，除法律法规另有规定外，收集使用个人信息应当征得信息主体同意。根据《网络安全法》第七十六条第（五）项，个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。据此，个人信息的认定应当采取直接识别和间接识别相结合的认定标准。《民法典》第一千零三十四条对个人信息的定义也采用了相同的认定方式。

作为《网络安全法》的配套标准，《信息安全技术 个人信息安全规范》（GB/T 35273-2020）（以下简称《个人信息安全规范》）附录 A1 所列举的个人信息包括个人上网记录，如通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等。

虽然我国目前的法律框架对 Cookie 的规定不像欧盟那样细致全面且直接，但从遵守与个人信息保护相关的法规要求中还是可以找到相关答案的，包括：

1. 公开收集、使用规则，明示收集、使用信息的目的、方式和范围；

2. 征得用户的同意（如信息主体为儿童，则应征得其监护人同意），未经被收集者同意，不得向他人提供个人信息；

3. 遵循最小必要的原则，只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量；

4. 向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等方法；

5. 采取技术措施和其他必要措施，确保收集的个人信息安全，防止信息泄露、毁损和丢失。

2020 年出台的《中华人民共和国个人信息保护法（草案）》（以下简称“《个保法（草案）》”）也对前述的原则性规定作出了进一步明确，但与《民法典》、《网络安全法》与《个人信息安全规范》要求以“同意”作为唯一合法事由相比，《个保法（草案）》借鉴了 GDPR 第六条的体例，将日常生活中可能出现的另外五类情况（例如履行合同所必需、履行法定职责所必需、维护公共利益等），与个人信息主体的“同意”并行放置，

作为处理个人信息的合法依据。只要企业能够证明自己具有《个保法（草案）》要求的合法性基础，又履行了基本的合规义务，即能够满足合规要求，这样给予企业在无法拿到“同意”时，更加灵活以及自我控制风险和自证合规的做法。同时，《个保法（草案）》对同意的形式进行了具体要求，即应当由个人在充分知情的前提下，自愿、明确地作出意思表示。

此外，《个保法（草案）》还提及了“单独同意”的表述，适用场景包括向第三方进行提供（第二十四条）。这将适用于使用第三方 Cookie 时可能涉及到共享用户个人信息的情况。但是，鉴于《个保法（草案）》目前并非生效，企业可以优先参照《网络安全法》和《个人信息安全规范》的同意标准，且提前为《个保法（草案）》的其他合法事由做好准备。

（二）典型 Cookie 案例

2013 年，被称为 Cookie 技术与隐私权纠纷第一案的朱某诉百度 Cookie 案中，原告朱某在利用家中和单位的网络上网浏览相关网站过程中，发现利用“百度搜索引擎”搜索相关关键词后，会在特定的网站上出现与关键词有关的广告。朱某认为，百度公司利用网络技术，未经朱某的知情和选择，记录和跟踪了朱某所搜索的关键词，将朱某的兴趣爱好、生活学习、工作特点等显露在相关网站上，并利用记录的关键词，对朱某浏览的网页进行广告投放，侵害了朱某的隐私权，使朱某感到恐

惧和精神高度紧张，影响了正常的工作和生活，故诉至法院，请求判令百度公司立即停止侵害朱某隐私权的行为，并赔偿朱某精神损害抚慰金10,000 元。

法院经审理查明，百度公司个性化推荐服务的技术原理是：当网络用户利用浏览器访问百度网站时，百度网站服务器就会自动发送一段Cookie 信息存储于网络用户的浏览器中。通过建立 Cookie 联系后，百度服务器会对用户通过浏览器浏览的网页内容进行技术分析，并推算出使用浏览器一方可能的个性化需求，再基于此种预测向该浏览器的不特定使用人提供个性化推荐服务。

一审法院认为，个人隐私除了用户个人信息外还包含私人活动、私有领域。朱某利用三个特定词汇进行网络搜索的行为，将在互联网空间留下私人的活动轨迹，这一活动轨迹展示了个人上网的偏好，反映个人的兴趣、需求等私人信息，在一定程度上标识出个人基本情况和个人私生活的情况，属于个人隐私的范畴。百度公司使用 Cookie 技术收集了原告朱某的网上活动轨迹，并根据朱某的上网信息，在与百度公司合作的网站上展示了与朱某上网信息有一定关联的广告推广内容，是进一步利用了他人隐私进行商业活动的行为，构成侵犯他人隐私权行为。[31]可

[31] （2013）鼓民初字第 3031 号。

以看出，一审法院认可用户的网络活动踪迹具有隐私属性，但是并未明确认定搜索关键词等 Cookie 信息是否属于个人信息。[32]

二审法院认为，百度公司在提供个性化推荐服务中运用网络技术收集、利用的是未能与特定网络用户个人身份对应识别的数据，该数据的匿名化特征不符合“个人信息”的可识别性要求。二审法院对 Cookie 信息是否属于个人信息的判断，依据的是国家工信部《电信和互联网用户个人信息保护规定》对个人信息的界定。根据该规定第四条，个人信息是指电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的网络用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户以及网络用户使用服务的时间、地点等信息。二审法院认为，网络用户通过使用搜索引擎形成的检索关键词记录，虽然反映了网络用户的网络活动轨迹及上网偏好，具有隐私属性，但这种网络活动轨迹及上网偏好一旦与网络用户身份相分离，便无法确定具体的信息归属主体，不再属于个人信息范畴。百度公司个性化推荐服务收集和推送信息的终端是浏览器，没有定向识别使用该浏览器的网络用户身份。[33]

---

[32] 王融：“反转的法律天平 我国 Cookie 隐私第一案判决”，《现代电信科技》，2015 年。.

[33] （2014）宁民终字第 5028 号。判决原文摘录：“个性化推荐服务客观上存在帮助网络用户过滤海量信息的便捷功能，网络用户在免费享受该服务便利性的同时，亦应对个性化推荐服务

百度 Cookie 案的判决引发了较大争议，有学者提出，个人信息的可识别性不仅包括“直接识别”，也包括“间接识别”，应当考虑用户的网络活动踪迹与其他信息结合时所具有的识别可能性。[34]据此，从学界角度，可能更倾向于将 Cookie 信息定义为个人信息的范畴。

2014 年，在顾俊与奇智软件（北京）有限公司、北京奇虎科技有限公司隐私权纠纷判决[35]中，原告认为 360 安全浏览器 5.0 正式版软件收集并上传了其计算机中是否安装了 QQ 管家、金山毒霸、搜狗输入法、QQ、搜狗浏览器、遨游浏览器、Firefox 浏览器、Chrome 浏览器、360 极速浏览器、QQ 浏览器、百度浏览器、阿里云软件的信息，构成了对原告隐私权的侵害。对此，法院认为，隐私权是指自然人享有的对其个人的、与公共利益无关的个人信息、私人活动和私有领域进行支配的一种人格权，原告对其上述软件安装信息的隐私属性举证说明尚不充分。该类软件均为计算机使用过程中的常见软件，并不具有一般的人格或身

的不便性持有一定的宽容度。本案中，百度网讯公司的个性化推荐服务的展示位置在合作网站的网页，只有网络用户控制的浏览器主动登录合作网站时才会触发个性化推荐服务，并非由百度网讯公司或合作网站直接向网络用户的私有领域主动推送个性化推荐服务。即便没有开展个性化推荐，合作网站也会在其网页上进行一般化推荐。百度网讯公司的个性化推荐利用大数据分析提高了推荐服务的精准性，推荐服务只发生在服务器与特定浏览器之间，没有对外公开宣扬特定网络用户的网络活动轨迹及上网偏好，也没有强制网络用户必须接受个性化推荐服务，而是提供了相应的退出机制，没有对网络用户的生活安宁产生实质性损害。”

[34] 王融：“反转的法律天平 我国 Cookie 隐私第一案判决”，《现代电信科技》，2015 年。

[35] （2014）浙杭民终字第 1813 号。

份属性，故即使原告证明了 360 安全浏览器 5.0 正式版软件确实存在上述收集并上传的行为，360 安全浏览器也无从判断顾俊的真实身份及其人格特性，因此原告的隐私权并未因此受到侵害。

而在 2017 年陈鱼与杭州阿里妈妈软件服务有限公司网络服务合同纠纷案[36]中，原告诉请法院判定被告收集 Cookie 记录侵犯用户隐私权，法院并未直接判断 Cookie 记录是否属于个人信息，而是从同意的角度出发，认为被告收集 Cookie 记录已获得原告同意，因而不侵犯隐私权。

在该案中，原告在被告阿里妈妈公司运营的“阿里妈妈”网站申请注册了淘宝客账户。随后，原告利用自己注册的 www.qnjjt.com 域名搭建了内含多个页面的导航平台网站用以淘宝客的推广业务，即网络用户通过该导航平台网站的不同页面可进入相应的“淘宝”、“天猫”等购物平台进行浏览和购买，从而原告可对交易订单的金额提取一定比例的佣金。2017 年 6 月，被告通知原告，因原告运营的导航平台网站流量异常，冻结了原告的淘宝客账户。原告因此诉至法院，要求被告立即解冻。此外，原告还提出被告阿里妈妈公司作为服务提供商，收集用户 Cookie 记录涉及侵犯用户隐私权和服务协议的约定。

针对被告收集 Cookie 记录侵犯原告隐私权这一争议焦点，法院认

[36] （2017）浙 8601 民初 3306 号。

为，根据《阿里妈妈服务协议》5.1 个人信息条款的约定，用户在使用阿里妈妈提供的服务时，同意被告收集其 Cookie 记录。同时被告阿里妈妈公司作为服务提供商，负有管理职责，需要根据 Cookie 记录对原告等淘宝客进行流量监管、费用结算。原告等在内的用户点击确认《法律声明等隐私权政策》，同意被告收集其 Cookie 记录，故被告收集 Cookie 记录是在用户同意授权的情况下进行的，用户可以根据自己的偏好管理或删除 Cookie，也可以清除计算机上保存的所有 Cookie，所以被告阿里妈妈公司在本案中使用 Cookie 有合理性，原告诉称被告收集用户 Cookie 记录侵犯隐私权，不能成立。

基于上述三个典型案例，可以发现，在《民法典》、《网络安全法》等相关法规出台前， Cookie 相关的案例总体来说主要是从侵犯隐私权的角度出发 ,法院趋向于认为 Cookie 不属于隐私或者个人信息的范畴。而随着百度 Cookie 案中 Cookie 信息是否属于个人信息这个存在争议问题的讨论，2017 年《网络安全法》的实施和《个人信息安全规范》以及《民法典》的出台，Cookie 是否属于个人信息已经得到了解答。

七、关于国内、外平台 Cookie 合规情况的调研

（一）关于外观展示上的调研

为了在储存 Cookie 收集信息前履行告知同意的义务，在实践中，

网站往往通过 Cookie Banner、控制面版以及 Cookie 声明向用户告知有关 Cookie 信息并获取用户同意。我们对国内外网站的相关实践情况进行了调研，相关情况如下：

1. 国外网站（以欧盟为例）

（1）Cookie Banner

图 1 OneTrust Dataguidance 官网的 Cookie Banner

通常，网站通过 Cookie Banner（“横条”）来获取用户同意。在 Cookie Banner 中明确告知用户使用 Cookies 的各类目的以及同意的后果，直接赋予了用户管理 Cookie 的权利。

德国等欧盟成员国的数据监管机构认为，使用横条征得用户同意是现有的技术水平，经合理设计的能够证明 GDPR 合规的一种方式。但是，

须注意的是，对于利用 Cookie 征得用户同意的方式仍存在不确定之处，目前没有定论，留待未来的判例和 E-PR 进行进一步确定。我们初步将征得同意的要求总结如下：

- 原则上，如果用户拒绝使用 Cookie，网站不得以此为由拒绝该用户使用网站。拒绝使用 Cookies 应当仅导致部分功能不能实现。
- Cookie Banner 不得妨碍用户访问网站的用户服务协议、版权声明和隐私声明，并应当附上 Cookie Statement、Privacy Statement 的链接。
- Cookie 横条不仅应当向用户提供同意追踪的选项，也应当提供拒绝追踪的选项。同意的按钮设计不应当比拒绝的按钮在位置和技术实现方式上更显眼或方便。此外，不得默认同意，例如预先勾选相应的复选框。
- 必须向用户提供“同意”或者“拒绝同意”Cookie 的选择。譬如，根据德国数据监管机构发布的指南，必须对每一个 Cookie 单独提供“同意”或者“拒绝”的选择。然而，在实践中常见的方式为仅对部分 Cookie 提供单独同意或拒绝的选项，例如分析类 Cookie，市场营销类 Cookie。
- 当用户点击“禁用所有（Disable All）”时，可保持非必要的 Cookie 处于禁用状态。用户是否点击“允许所有（Allow All）”不影响其

正常浏览网页。

- 如果用户未作任何点击动作而继续浏览网站并不视为授予了同意。

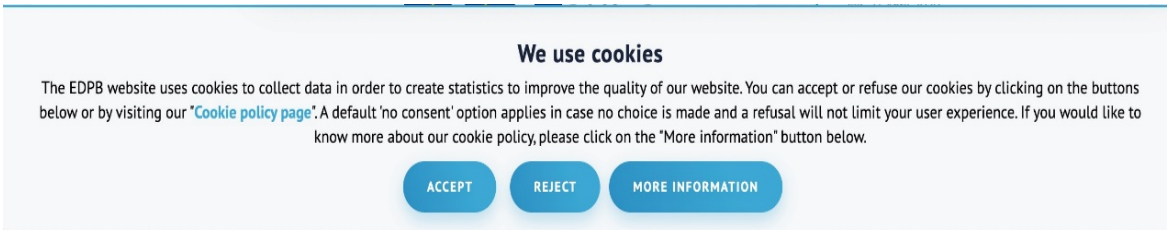

图 2 EDPB 网站征求用户同意时使用的两层设计结构

如上图所示，我们建议在征得用户同意时，可采取两层设计的结构：

➢ 第一层

在访问网站时，所有的 Cookies 均不应事先存储于客户端，所有的同意勾选框均为空白（即非默认勾选状态），并在页面上展示 Cookie 横条，在 Cookie 横条内提供“接受 Cookie”、“拒绝 Cookie”以及“Cookie 的个性化设置”三个选项。

➢ 第二层：

- 如果用户选择“接受 Cookie”，则所有的 Cookies 均被激活，所有的同意框均被勾选，且公司应当对用户的同意进行记录；
- 如果用户选择“拒绝 Cookie”，则所有的 Cookies 均未被激活，所有的同意框仍然处于未勾选的空白状态；
- 如果用户选择“Cookie 的个性化设置”，则展示第二层页面，即“Cookie 控制面板”，允许用户勾选不同类型的 Cookies。

（2）Cookie 控制面板

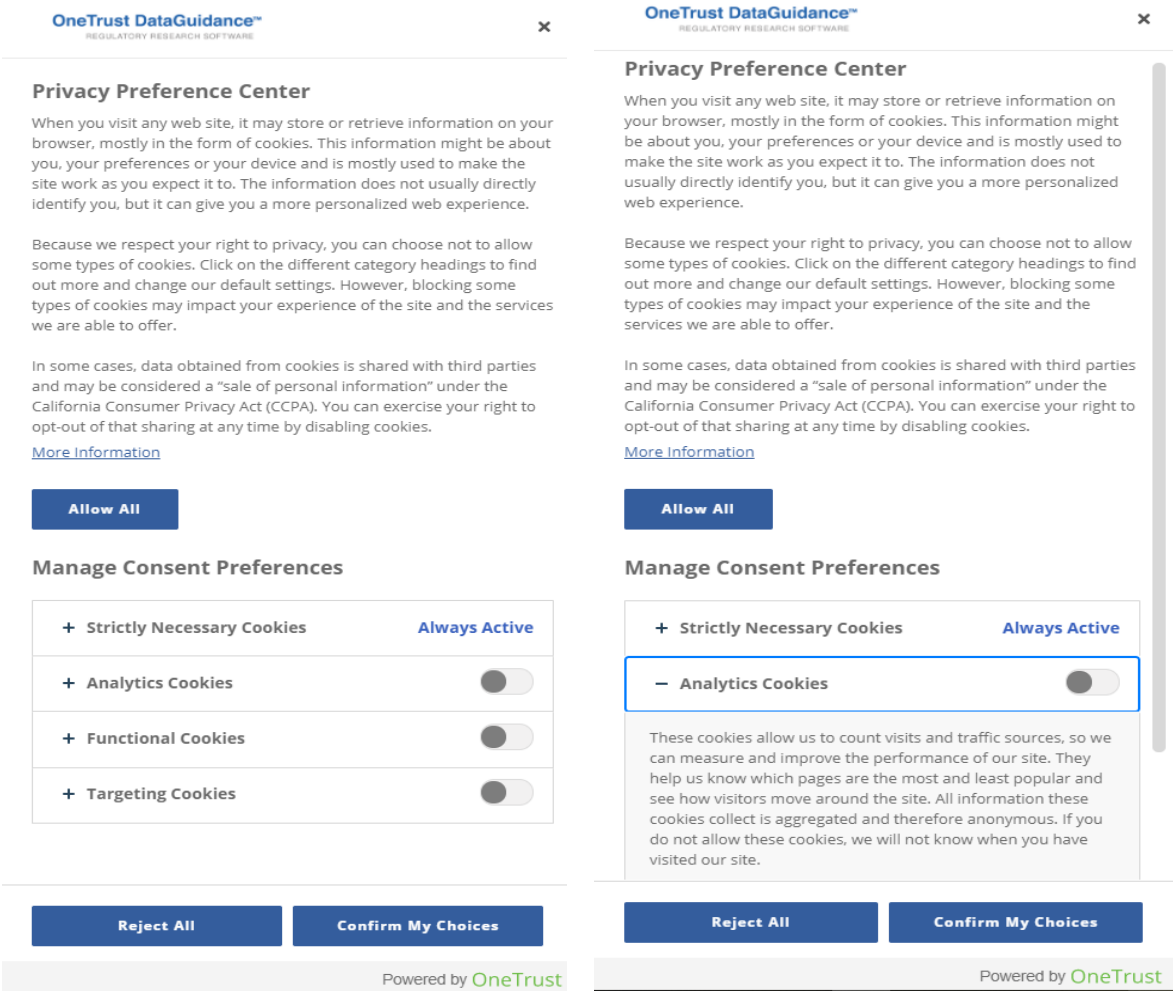

图 3 OneTrust Dataguidance 官网的 Cookie 控制面板

从 Cookie 横条点击“Cookie Setting”（Cookie 的个性化设置）进入后，通常网站提供了查看其所用 Cookie 的控制面板，用户可以通过该面板勾选/滑向同意或撤回对于不同种类 Cookie 的授权同意。同时，该面板还应当对网站使用 Cookies 的情况做出了进一步的说明，并且需要为用户较为详细地说明各类 Cookies 的具体目的以及运作方式。此外，对于技术必需型 Cookie，可以未经数据主体的同意进行使用，常见的技术必需型 Cookie 可能包括临时 Cookie、验证 Cookie、多媒体

内容播放临时 Cookie（例如 flash player Cookie），以及负载平衡临时 Cookie 等。对于其他 Cookie，原则上，公司只有征得用户同意才能使用。常见的需征得用户同意才能使用的 Cookies 包括：Google Analytics、Google AdWords、Facebook Custom Audiences、LinkedIn Insight Tag 等。

如果为了说明 Cookie 存在正当利益时的使用，公司一般须证明：

- 使用 Cookie 具有正当利益；
- 使用 Cookie 收集数据是为了实现正当利益（现实中存在争议，DPA 可能会认为，为确定网站用户的数量而将数据传输给第三方社交媒体和外部分析服务提供者是不必要的，因为为实现这一目的可以采用其他方式，例如内置分析软件等）；
- 公司使用 Cookies 的利益大于网站用户的利益。

理论上讲，网站运营者还需要对每一个 Cookie 进行详细的、全方位的利益平衡分析，包括使用 Cookie 对用户的干扰、用户的合理期待，所涉及的数据、被处理数据的规模、类型、处理者身份等。

此外，所有非绝对必要种类的 Cookie 开关都需要默认关闭，即相应 Cookie 都是默认禁用的。如前所述，网站运营者需要向用户提供同意所有类型 Cookie 的选项，另一方面也需要提供能够确拒绝某些

Cookie 的选项。

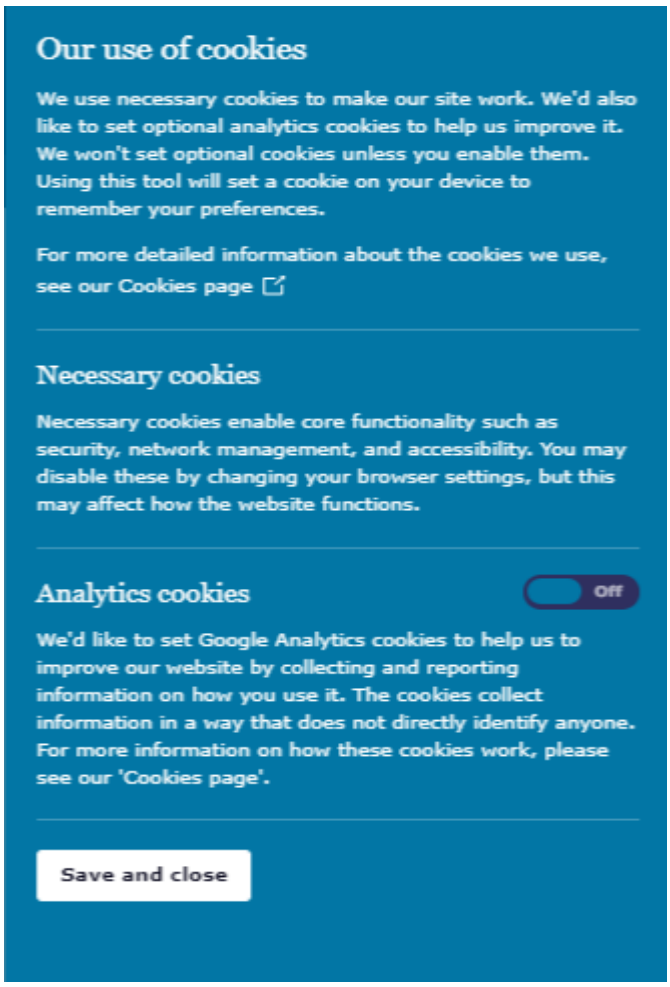

图 4 ICO 的 Cookie Banner 对非技术必需型 Cookie 设置了由用户选择同意其他 Cookie 的选项

（3）Cookie 声明

除了设置 Cookie 横条以及 Cookie 控制面板外，同样需要向网站用户告知通过 Cookie 收集信息的情况。因此，应当在 Cookie 横条和/或控制面板上附上 Cookie Statement 或包含对 Cookie 描述的 Privacy Policy 或类似文件的链接。

以下为 Cookie Banner 的示例，图片来自英国数据保护机构的官网。

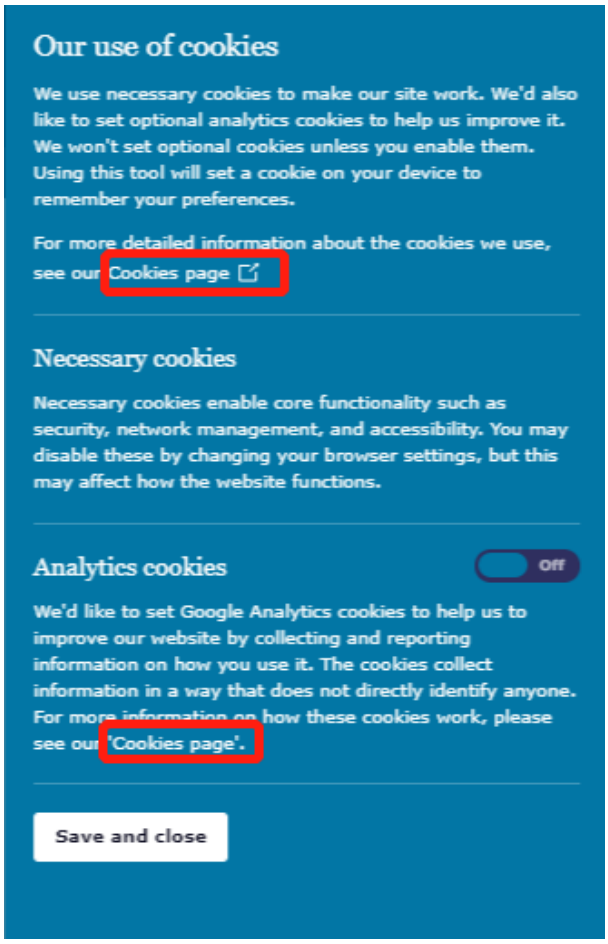

图 5 ICO 的 Cookie Banner 附上了 Cookie Page 的链接

从企业的良好实践来看，有些网站在 Cookie 声明中除了对于 Cookie 及类似追踪技术进行了介绍之外，还告知了用户对 Cookie 进行设置管理的方式。譬如，下述网站还提供了其所用 Cookie 的详细分类清单，并说明了每类 Cookie 的作用以及禁用的后果，同时也列出了 Cookie 的名称、使用方式和存储期限等详细信息，并且还能够提供用户选择删除 Cookie 和 Cookie 记录的选项。

Cookie List

A cookie is a small piece of data (text file) that a website – when visited by a user – asks your browser to store on your device in order to remember information about you, such as your language preference or login information. Those cookies are set by us and called first-party cookies. We also use third-party cookies – which are cookies from a domain different than the domain of the website you are visiting – for our advertising and marketing efforts. More specifically, we use cookies and other tracking technologies for the following purposes:

Strictly Necessary Cookies

These cookies are necessary for the website to function and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as setting your privacy preferences, logging in or filling in forms. You can set your browser to block or alert you about these cookies, but some parts of the site will not then work. These cookies do not store any personally identifiable information.

Cookie Subgroups	Cookies	Cookies Used	Lifespan
dataguidance.com	OptanonConsent, _dc_gtm_UA-xxxxxxxx, __cfduid	1st Party	365 Days, 0 Days, 30 Days
corporate.dataguidance.com	OptanonAlertBoxClosed	1st Party	365 Days
onetrust.com	__cfduid	3rd Party	0 Days

Analytics Cookies

These cookies allow us to count visits and traffic sources, so we can measure and improve the performance of our site. They help us know which pages are the most and least popular and see how visitors move around the site. All information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies, we will not know when you have visited our site.

Cookie Subgroups	Cookies	Cookies Used	Lifespan
dataguidance.com	_gid, _ga	1st Party	1 Days, 730 Days

Functional Cookies

These cookies enable the website to provide enhanced functionality and personalisation. They may be set by us or by third party providers whose services we have added to our pages. If you do not allow these cookies then some or all of these services may not function properly.

Cookie Subgroups	Cookies	Cookies Used	Lifespan
www.dataguidance.com	has_js	1st Party	Session

图 6 列举所用 Cookie 的详细分类清单

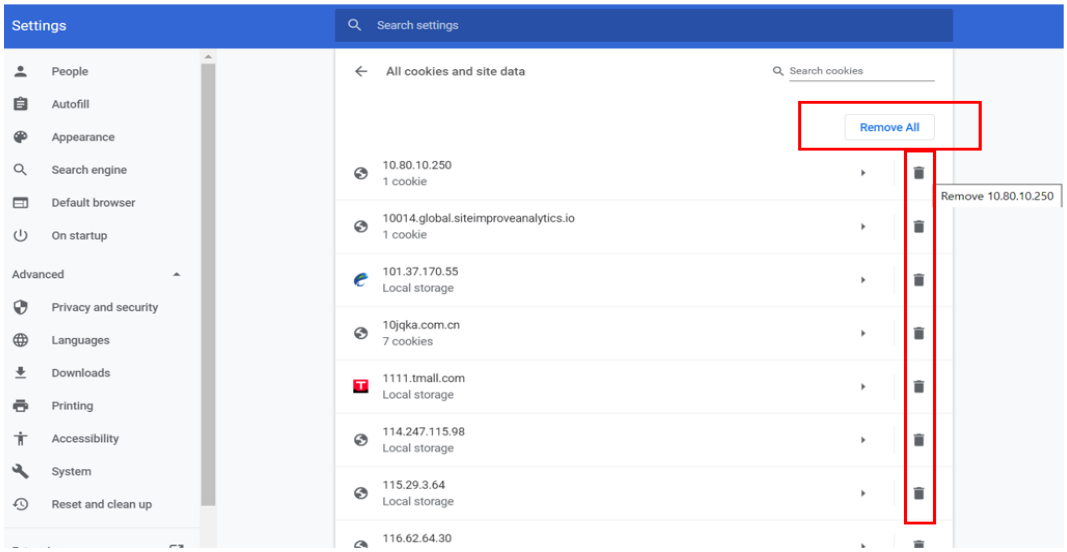

图 7 提供用户选择删除 Cookie 和 Cookie 记录的选项

（4）Cookie 白名单/黑名单设置

欧盟 E-PR 推荐了通过浏览器进行设置，以避免频繁的同意请求对用户造成过度的打扰。诸多浏览器已经提供此类设置，如下图谷歌 Chrome 浏览器，提供了用户可设置“一直允许使用 Cookie”和“完全不允许使用 Cookie”网站名单的机制，用户可根据自己的偏好进行设置。

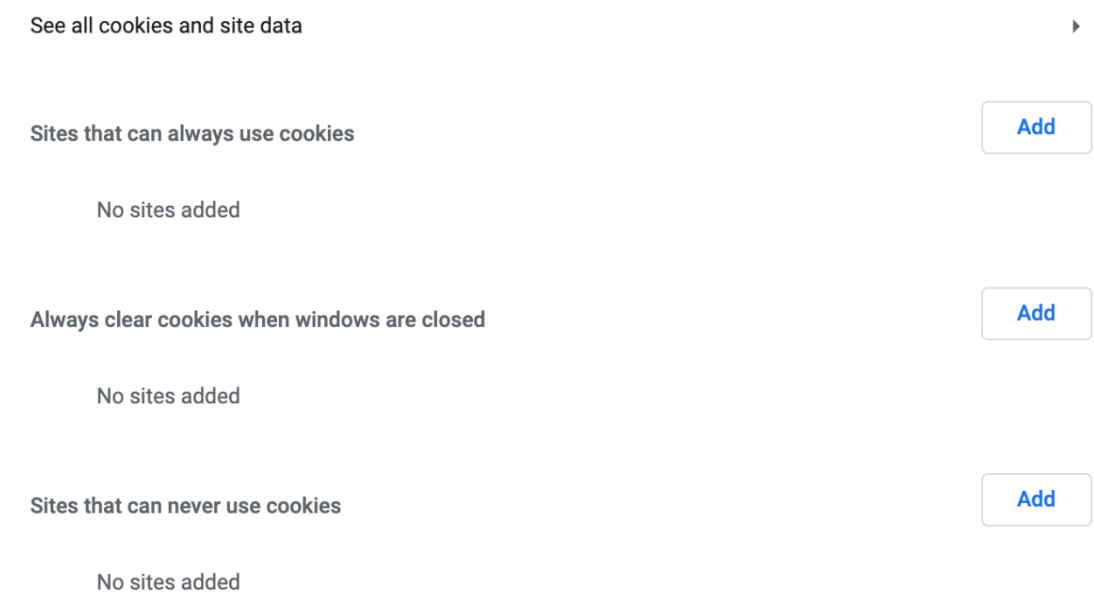

图 8 Chrome 浏览器中对于 Cookie 进行设置的页面

2. 国内网站

（1）案例一：中国某科技巨头线上商城官网

图 9 某科技巨头线上商城官网 Cookie Banner

在 Cookie Banner 中告知用户使用 Cookie 的具体目的，仅提示用户其会使用 Cookie 技术。用户是否关闭此提示不影响其浏览及使用相应服务。用户关闭此提示后，再重新登入官网时，此提示不再显示。

在 Cookie Banner 中简要介绍了使用 Cookie 的具体目的，用户是否关闭此提示不影响其浏览及使用相应服务。用户点击相应选项或关闭此类提示后，当用户重新登入官网时此类提示不再显示。

（2）案例二：中国某国际航空公司

图 10 中国某国际航空公司 Cookie Banner

在 Cookie Banner 中直接赋予了用户管理 Cookie 的权利，当用户点击 Cookie 设置时，可自行选择开启或禁用相应 Cookie，除必要的 Cookie 外，用户均可选择禁用。用户是否点击“接受所有 Cookies”不影响其正常浏览网页。

（3）案例三：某跨国标准技术服务公司官网

图 11 某跨国标准技术服务公司官网 Cookie Banner

点击 Cookie 设置，出现的弹窗如下：

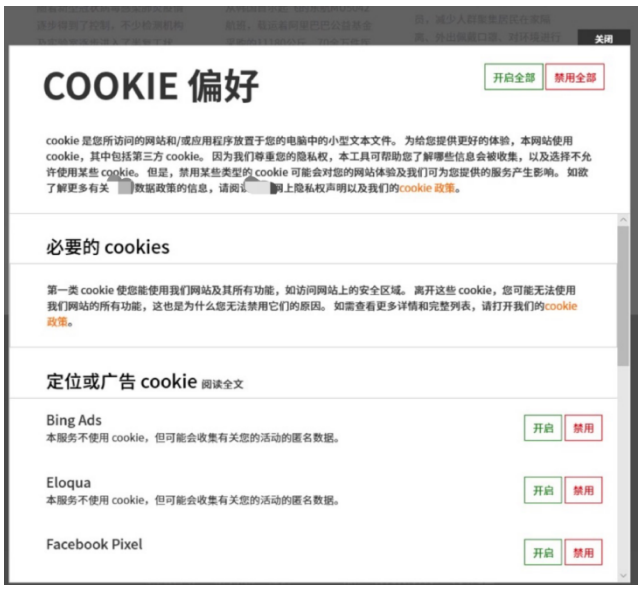

图 12 某跨国标准技术服务公司官网点击 Cookie 设置后的弹窗

用户可以选择“开启全部”或“禁用全部”非必要 Cookie，也可以对非必要 Cookie 进行逐项的选择“开启”或“禁用”。

（4）案例四：某知名奢侈品牌中国官网

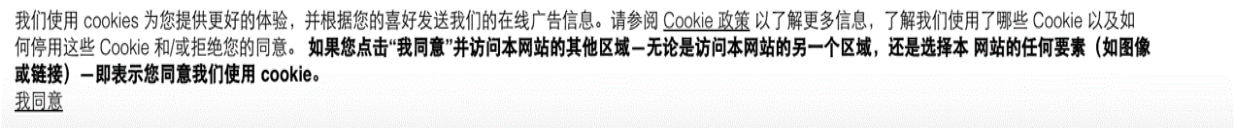

图 13 某知名奢侈品品牌中国官网 Cookie Banner

在 Cookie Banner 中解释了网页使用 Cookies 的具体目的及可能构成同意使用 Cookie 的行为逻辑，整体表述清晰。在 Cookie Banner 中同时嵌入了 Cookie 政策的链接 ,以使用户了解更多有关使用 Cookie 的信息。但 Cookie Banner 未设置可关闭的选项，用户如不同意，该 Banner 将持续展示。

（二）关于技术创新上的调研

在应用传统用户追踪技术的同时，国内外企业也在隐私备受关注的新形势下进行了技术和措施创新，旨在限制 Cookie 对用户隐私的影响并逐步探索新的技术手段取代 Cookie 的角色。

为应对第三方 Cookie 对用户的追踪，国际上的组织和公司出于隐私保护的理念，如前所述，已经提出了“禁止追踪”（Do Not Track）的概念，对第三方 Cookie 的使用场景进行了一定程度的限制。Do Not Track 的核心思想是 HTTP 协议的头字段将与访问 Web 页面的请求一同被发送，而该协议的头字段可以表明用户已经设置或做出选择请求不被追踪。Do Not Track 请求实际上并未自动阻止用户与特定追踪者之间的通信，因此用户希望不被追踪的请求实际需要依靠公司的操作来实现。由于 Do Not Track 概念的普及和用户对隐私越发的重视，在 2010 年前后浏览器软件几乎都提供了防止追踪识别的功能，且不断有新的应用与网站的插件，辅助用户不被网站过度追踪并收集信息。比如微软浏览器在 IE10 的版本中将 Do Not Track 设置为默认的选项。用户可以通过浏览器和插件，决定停止某些不必要的追踪和信息收集。但 Do Not Track 因为其含义和实现机制，在很大程度上无法实现最终意义的隐私

保护。[37]比如在用户删除 Cookie 的时候，包含其 Opt-Out 请求的 Cookie 也很有可能被一并删除；而且用户 Opt-Out 的请求在被处理时也很难做到立即有效。

此外，国内外企业还针对防止用户身份认证追踪行为做了一些新的尝试。谷歌于 2019 年 8 月推出了“隐私沙箱”计划，旨在开发一套开放标准，用于提升隐私和网络安全。在这一计划中，谷歌提出用多个项目和用例实现默认的隐私保护，其中包括以负责任的方式逐步移除第三方 Cookie 和用更为缓和的方式替代现有的跨站点追踪功能。[38]该计划展示的替代第三方 Cookie 的方案包括缓存检查（Cache Inspection）、链接装饰（Link Decoration）、网络级追踪（Network Level Tracking）等。而且在该计划下，当用户出于隐私保护的原因对谷歌浏览器的这些追踪或营销行为不满意或不喜欢时，用户可以方便地关闭相应功能模块。

近几年，“数据净室”（Data Clean Room）这一概念也开始被提及。数据净室是一个安全独立的平台，可链接来源于多方的匿名营销数据和广告数据。与其他数据共享的方法不同，数据净室虽然包含了详细

[37] 参见 IAPP_T_TB_Introduction-to-Privacy-for-Technology_1.1。

[38] 参见 https://www.chromium.org/Home/chromium-privacy/privacy-sandbox，最后访问日期 2021 年 2 月 18 日。

的广告展示数据，但在输出用户级结果时具有严格的隐私和安全限制。其通过将匿名数据进行安全整合以实现对目标用户市场的精准投放，而不再通过 Cookie 获取用户个体层面的数据而侵犯用户隐私。数据净室的一个主要形式是 Facebook、Amazon、Google 等网站的封闭式广告平台。这几个网站都采用这一方式来向品牌商提供其平台的广告数据。这些品牌商客户通过这些数据来评估广告的效果，并优化在该平台的广告方案。

为缓和实时竞价与广告技术中的主要争议--数据使用和数据隐私互相冲突问题，互联网架构委员会（IAB）曾提出了一种方案：要求第三方 Cookie 继续工作，就像它们现在在广告技术生态系统中所做的那样；同时，依赖于数百个市场参与者之间的合同承诺。因为 IAB 的方案并没有提出特定的技术保障措施，在实行上存在难度，2020 年 1 月 30 日，在数据和技术领域领先的 Anonos 公司与 Acxiom 公司，协同信息（利用）责任基金会（IAF）共同创立研究小组，提出了“the 5th Cookie”的概念。“The 5th Cookie”是一个比喻说法，它不依赖于第三方 Cookie，相反，它分配了一定数量的第一方 Cookie。这些第一方 Cookie 受到网站发布者的控制，并且和有限的受信任合作方进行合作使用。假设说这些受信任的合作方为（1）Facebook、（2）苹果、（3）亚马逊、（4）谷歌，以及（5）额外的一个或多个由利用了充分保障措施的“民主合作机

构”指定使用的 Cookie—这就是“the 5th Cookie”名称的由来。

“the 5th Cookie”通过《欧盟通用数据保护条例》（General Data Protection Regulation，以下简称“GDPR”）下的假名化与隐私保护设计、默认隐私保护的概念，建立与“同意差距”（Consent Gaps）进行连结的纽带。通俗点说，当数据处理的类型过于宽泛或者无法定义时（比如通过机器学习或者人工智能项目），“同意差距”就会出现，数据主体无法做出符合 GDPR 规定的有效同意来授权控制者对其数据进行处理。通过假名化与隐私保护设计、默认隐私保护相结合，可以缓和这一问题：假名化要求控制者在无使用分别存储的信息进行重新连接/重新识别数据主体的目的时，不能对主体进行重新识别，并且只能用于已授权的处理目的。同时，通过“可论证的问责制”对可审计且需记录的技术保障提供措施，使数据创新能够与个人权利的全方位保护保持平衡。

在此基础上，谷歌于 2021 年 1 月展示了一项名为 FLoC（Federated Learning of Cohorts）“联合学习群组”的新型 API，安装在 Google Chrome 中。通过终端设备机器学习（On-Device Machine Learning）的方式将用户分组，对具有共同兴趣的用户群组（具有相似的访问习惯等）进行广告推送。广告主接触到的数据主体是一个小型、动态变化并且尊重隐私保护的群体中成员，这个群体可以称为一个小区段（micro-segment）。每一个小区段代表了群体内的数据主体，并且根据个人的

特点，数据主体可以同时包含在多个小区段内。小区段的构成将会根据该小区段的固定特点进行动态变化。广告主可以由此接触他们感兴趣的用户群体，而数据主体不再是作为个体被接近，而是作为群体中的成员。

该新型 API 通过利用网页的 URL、网页的内容或网页的其他要素（而并非通过 Cookie）获取用户的访问行为信息，并将这些信息进行标签化处理，通过机器学习的方式进行分析。分析和广告推送的过程中不会涉及用于识别个体用户的信息标识符，不需要对特定用户的浏览记录进行跟踪，也不需要第三方 Cookie 的参与。关键是，数据主体可以随时选择退出基于市场营销和拓展进行的深度小区段。但该方案也存在一些实现上的弊端，比如会极大提升分析用户及投放广告的成本，也还在不断探索与研发中。

当第三方 Cookie 被禁，隐私监管日趋严格时，更成熟和更具针对性的技术手段代替 Cookie 在过去针对用户进行广告营销中的角色也在情理之中。一方面，企业要考虑是否能基于自己的网站或平台创建自身的用户数据分析机制，而不依赖于谷歌等第三方工具。将第一方 Cookie 和其他用户信息作为广告营销和投放的主要参考，在不侵犯用户隐私的前提下充分利用数据，将成为需要被重点考虑的问题。另一方面，网站所有者和广告平台或许可以携手，在充分尊重用户隐私的前提下打造新

的在线广告推送方案。[39]如数据净室、“the 5th Cookie”和“联合学习群组”的新尝试其实都是利用这一原理。在创新过程中，可以结合假名化、默认的隐私保护（Privacy Protection By Default）等技术方案，在算法中设置尽量完备的机制和参数，并给予用户合理的选择空间。

八、延伸思考：我国企业如何做好 Cookie 合规

（一）针对国内网站国内运营的 Cookie 合规

我国目前的法律体系主要是从个人信息保护的角度对 Cookie 进行规制。企业使用 Cookie 时应当确保遵循《网络安全法》、《个保法（草案）》中关于用户个人信息保护的相关规定，实际操作层面可以参照《个人信息安全规范》的具体细则。此外，需要指出的是，随着目前个人信息保护相关监管行动的增强，国内较多网站和 App 较多采用的是“阻断式”的隐私政策弹窗方案，要求用户在首次打开 App 时点击同意包含了 Cookie 声明在内的隐私政策，而没有根据产品的功能和特征为用户设置不同意隐私政策但仍能使用或提供仅浏览的选项。这在欧盟很有可能导致 Cookie Wall 的情况，并不被认为是合规的做法，建议根据产

[39] https://mp.weixin.qq.com/s/hCB6DZ6KAtrikDBlqGCkfw，最后访问日期 2021 年 2 月 18 日。

品的定位和类型区分判断是否向用户提供浏览模式及在此功能下的相关服务，并承诺如果涉及游客状态下个人信息收集的，应实践不做具体个人身份的识别，并确保在相对短的周期内（如一个月内）进行删除或者做匿名化处理。

图 14 国内某产品提供了仅浏览选项

图 15 国内某产品提供了删除 Cookie 缓存的选项

（二）针对出海业务的国内企业 Cookie 合规

在全球化背景之下，许多企业都有业务出海的需求，比如通过网站向境外售卖商品或者服务、提供 PC 端软件、提供移动端应用等，因此不少都会落入欧盟 GDPR 的管辖范围。不管我国未来是否会针对 Cookie 的合规进行很强的监管，不妨从出海业务开始，借鉴欧盟国家对于 Cookie 的法律要求和实践指南，从而在履行境外法合规义务的同时，对我国企业在国内网站的 Cookie 合规提供有益参考。因此，我们建议企业在 Cookie 合规方面注意以下几点：

首先，企业应当评估其所使用的 Cookie 是否为遵守法律要求或为用户提供其所要求的在线服务以及实现通信传输所必须的。若所使用的 Cookie 为非必要的，应当在使用 Cookie 之前征得用户同意。

其次，在征得用户同意方面，根据出海国家适用的数据保护法及直接营销等相关法规或 Cookie 指南（如 GDPR、《电子隐私指令》以及欧盟各国关于直接营销或者 Cookie 的具体规定，有效同意需要满足以明确肯定的行动、自由作出的、明确、具体、知情的同意。故建议企业：

1. 避免在获得用户明确同意前将 Cookie 存储到客户端；
2. 以 Cookie Banner 或特别提示、弹窗等方式单独征求用户同意使用 Cookie 而非将其捆绑在用户服务协议或者隐私政策当中；

3. 将 Cookie 横条以及 Cookie 政策的链接置于网页或者 App（当 App 使用 Cookie 或者类似技术时）的醒目位置，并确保首次浏览网站或者界面的用户能够轻易获取关于 Cookie 的相关信息；

4. 有单独的 Cookie 声明，详细说明网站/App 使用 Cookie 及类似技术的情况，包括对 Cookie 及类似技术的介绍、所用 Cookie 的名称、使用的目的、存续期限、类别、来源等，并向用户说明如何对网站所用的 Cookie 进行管理，即如何撤回和修改同意；

5. 避免使用“继续浏览网站即表示同意使用 Cookie”等消极方式获取用户同意，提供用户可以积极选择“接受”或“拒绝”的按钮，以及进一步能够向用户提供对 Cookie 进行分类细化管理的机制。此外，“接受”与“拒绝”的按钮在形状、大小上应当保持一致，以让用户可以清晰识别“拒绝”按钮，避免过于隐蔽；

6. 区分所使用的 Cookie 的类别：必要与非必要[40]。对于为了网站或者 App 运营必要的 Cookie，可以无须用户同意（例如身份验证 Cookie）；对于非必要的 Cookie（例如营销类 Cookie、分析

[40] “必要”Cookie 的常见类型可能有：会话 Cookie、身份验证 Cookie、以用户为中心的安全 Cookie（用于监测用户身份是否被滥用）、多媒体内容播放器会话 Cookie、负载均衡会话 Cookie、用户界面自定义 Cookie（例如语言或字体首选项）等。关于非必要 Cookie 的确切范围，各国监管机构的意见并不完全统一。

类 Cookie），则必须征得用户的主动同意才能开启。在页面设置上也可以采取一级与二级页面的方式。在一级页面上，告知用户使用 Cookie 的情况并放置同意、不同意与自定义（Customize）按钮和 Cookie 政策；在二级页面上，展示使用的所有的 Cookie，并提供用户可以开启或关闭各类非必要 Cookie 的按钮；

7. 若网站设置第三方 Cookie，则建议企业：

（1）以上述方式向用户提供关于第三方 Cookie 的信息并征得用户同意；

（2）以合同等方式明确与第三方之间关于征得用户同意、数据控制权、数据处理权限等方面的责任分配；

（3）当第三方 Cookie 提供者位于境外，应额外遵循 GDPR 项下对于数据出境的规定，与第三方 Cookie 提供者签署标准合同条款（Standard Contract Clause）等；

（4）确保第三方对用户个人信息的收集、使用、安全保障等符合法律要求，对第三方 Cookie 的收集处理行为进行审计监督，发现第三方违反法律规定或约定收集处理个人信息的，及时终止与第三方的合作关系。

8. 参考法国做法，至少每 6 个月重新征得用户对 Cookie 的同意。

九、附录——欧洲四国 Cookie 指南比较

国家 / 法规要求 / 要素	英国 2019 年《ICO Cookie 指南》	法国 2019 年《CNIL Cookie 指南》 2020 年《CNIL Cookie 建议（草案）》 《法国数据保护法》	德国 《有关在线跟踪技术的指南》	希腊 《HDPA Cookie 指南》	差异
严格必要的 Cookie （使用该 Cookie 是为用户提供网站服务的技术需求，否则网站或网站某些关键功能将无法运行）	（1）仅出于通过**电子通信网络**进行通信传输的目的（即通信豁免 communication exemption）；或者 （2）严格按照用户或用户要求**提供信息社会服务所必要**的 Cookie（即严格必要豁免 strictly necessary exemption） 以上两项可豁免事先同意的要求，适用其他法律依据。 其中，值得注意的是，上	《CNIL Cookie 指南》指出，符合下列条件的 Cookie 属于必要 Cookie，使用该类 Cookie 无需以同意作为法律依据： （1）单纯的技术型 Cookie； （2）是为用户提供在线服务所必需的（如进行身份验证等）。 CNIL 特别指出，仅用于计算网站或应用程式用户，以衡量网站或应用程式有效性或进行技术优化等的 Cookie 应该被认定为是网站或应用程式运营所必须的，无需获得用户同意。	N/A	（1）Cookie 仅用于通过电子通信网络进行的通信传输；或 （2）Cookie 仅是为了提供用户或用户明确要求的信息社会服务所严格必要的。	各国监管机构关于严格必要与非必要 Cookie 的确切范围的意见并不完全统一，例如对于分析类 Cookie（analytics Cookie）的认定。 分析类 Cookie 指的是在线服务提供者为收集用户的网站访问信息而使用的 Cookie，如网站上的用户数量、用户在网站上停留的时间以及用户访问网站的具体部分，上述操作通常被称之为“网络受众群体评

	述（2）项的豁免情形意味着存储（或访问）信息应该必不可少的，而不是合理必要的。因此，（2）项豁免的适用范围很窄，仅限于以下两种情形： 1）是为提供用户所要求的服务所必需的； 2）遵守法律的要求。				估”（web audience measurement）。 《ICO Cookie 指南》认为分析类 Cookie 并不符合“严格必要”的豁免情形，因此使用分析类 Cookie 需要征得用户有效同意。相比较，《CNIL Cookie 指南》认为，在特定条件下，受众测量和分析类追踪技术可以豁免同意。
豁免获得用户同意的情形	符合豁免情形的 Cookie，例如： （1）用于记住用户在结帐时希望购买的商品或将商品添加到“购物车”的 Cookie； （2）遵守 GDPR 安全原则所必须的 Cookie； （3）通过在多台计算机之间分配工作负载	用于记录用户对于使用 Cookie 的选择的 Cookie； （1）用于进行认证的 Cookie，包括用于确保认证机制安全运行的 Cookie； （2）为了最终计算消费金额或用于记录购物车详情的 Cookie； （3）用于进行 UI 交互设置的 Cookie（如语言设置等）； （4）通讯服务中用于保存负载	分析类 Cookie 如不涉及向第三方传输数据则不需要获得用户的同意。	符合豁免情形的 Cookie，例如： （1）用户输入的 Cookie (session-id)； （2）用于身份验证的 Cookie； （3）以用户为中心的安全 Cookie（如用于检测认证滥用）； （4）为了保持网页以用户偏好方式（如语言设	请参见左侧表格。

	来帮助确保快速有效地加载页面内容（通常称为“负载平衡”或“反向代理”） 的Cookie。 根据公平原则和透明度要求，满足豁免事先同意要求的 Cookie 仍然需要向用户告知有关该 Cookie 的全面且明确的信息。	平衡的Cookie； (5) 用于设置付费墙的Cookie，以限制对于网站的免费访问； (6) 部分符合条件的分析类Cookie。		置、搜索历史等）展示的Cookie； （5）用于在某个特定会话中保持负载平衡的Cookie。	
非必要 Cookie	**分析类 Cookie** 不符合豁免同意的条件，属于非必要 Cookie。尽管分析类 Cookie 可以为在线服务提供者提供有用的信息，但它们并不是为提供用户所要求的在线服务功能所必须的。因此分析类 Cookie 需要征得用户同意。	加强了同意有效性的要求，有效同意必须是用户以“明确肯定的行动”所表示出来的同意；因此，用户继续浏览网站的行为不构成有效同意。另一方面，企业必须能够证明他们确实已获得用户的有效同意。因此，CNIL 建议将用户同意或拒绝的选择记录保存 6 个月。 使用了第三方来对 Cookie 进行管理的内容出版商仍被视为数据控制者。	N/A	任何在技术上不被认为是网络通信或提供用户要求的网络服务所必要的追踪技术的使用都需提前征得用户同意；且在任何情况下，无论是否必要，都应就使用跟踪技术向数据主体进行通知（notice）。 提供在线广告服务的 Cookie 和进行 web 分析 Cookie 不属于上述豁免范围，以上两类只有在用户知情同意的情况下才能使用。	法国认为，分析 Cookie 不总是需要事前同意，某些分析型 Cookie，如符合 CNIL 的规定，可获豁免事先同意的规定。 英国认为，所有的分析类 Cookie 都需要获得事前同意，无一例外。

告知的形式和内容	应向用户告知“明确和全面的信息”，考虑用户的认知水平，确保所提供的信息对于所有人而言都是可理解的。一般而言，提供在网站上运行的所有Cookie的详细列表可能是符合要求的方式。 具体而言，企业需要向用户告知有关 Cookie 的全面清晰的信息，包括使用 Cookie 的目的和持续时间。在提供相关信息的方式上，需要注意： (1) 使用户在首次访问在线服务时即可以看到相关信息； (2) 在隐私政策或 Cookie 政策中提供有关 Cookie 的更详细信息； (3) 在线服务的设计应当使得提供 Cookie 信息的链接具有显	向用户提供有关使用Cookie的目的，以及防止此类存储或访问的方法的信息。	可采取 Cookie 横条的形式来获得用户的有效同意，在Cookie横条展示期间，数据控制者应确保不收集任何个人数据。应向用户透明且全面地告知有关数据处理的所有类型、所有数据接收者的细节。	推荐网站使用恰当的机制告知相关信息并征求用户同意（如弹出式窗口或横条）。 横条（不论是弹窗还是其他形式）应该对每个追踪技术的目的进行详细说明。针对每一个追踪技术或追踪技术种类，告知内容应该包括数据处理的持续时间、数据控制者的身份、接收者的身份或接收者的类别。	目前各国基本均要求进行明确和全面的告知，说明Cookie的使用目的等。

	著性。例如，简洁网页底部没有“折叠”的链接将比放在字数更为密集的网页的页脚中的链接更具有显著性。其他提高 Cookie 信息显著性的方法包括： i. 格式：包括更改链接的大小或使用其他字体。关键是使得指向有关 Cookie 的信息与其他链接区分开； ii. 位置：将链接从页面页脚移动到更容易引起注意的位置； iii. 措辞：使得链接的名称包含一些说明性的文字，而不仅仅是将其命名为“隐私政策”（比如“了解有关我们网站的工作方式以及我们如何使您控制您的更多信息。”）				

		iv. 语言：根据网站受众使用合适的语言，不要使用冗长和过于复杂的术语。				
有效同意的要件	**事先同意**	企业必须确保在征得用户同意之前不得使用任何非必要 Cookie。企业不得预先启用任何非必要的 Cookie，因为这剥夺了用户的选择权。 例如，网站在其登录界面上设置了非必要 Cookie，其使用诸如“继续使用我们的网站即表示您同意我们使用 Cookie”之类的措辞，即使该界面还包含“确定”或“接受”按钮，也不被视为有效同意。这是因为该网站已决定设置非必要 Cookie，然后再寻求用户的同意，其只是向用户提供了“继续”的选项，而不是为用户“接受”或“拒绝”Cookie 提	CNIL 强调了《电子隐私指令》第 5 条第 3 款规定，即（在用户终端的）读写操作必须系统地经过用户的事先同意，并告知用户。 同时《CNIL Cookie 指南》强调，为了确保透明度，用户应有权知晓上述 Cookie 的设置情况和目的，企业可以在隐私政策中对此进行披露。	Cookie 及其他所有能够存储或访问用户设备信息的技术（如 pixels，SDK 等）都应遵守指南中所明确的要求。	Cookie(或类似技术)可用于存储信息或访问存储在用户/用户技术设备中的信息，前提是用获得用户的同意。	在合法性基础方面，和英国不同的是，法国未明确同意是处理个人信息的唯一合法性基础。 英国方面则认为，合法利益(legitimate interest)不是处理与 Cookies 有关的个人数据的适当法律依据。在已经有符合 GDPR 的同意的情况下，依靠合法利益是没有必要的，而且会给用户带来困惑。

		供了自由选择。				
	同意的自由性	“Cookie 墙”不符合 GDPR 关于同意自由性的要求。ICO 指出，通过 Cookie 墙强制获得的同意“不太可能有效”。然而，报告也指出，GDPR 必须与其他权利相平衡——包括言论自由和经营业务的自由。ICO 似乎对此持观望态度——至少目前如此。	只有数据主体可有效地做出选择且在没有给出同意或者撤回同意时不会遭致重大不便时，同意才是有效的。 **CNIL 同时提出了以下实操指引：** 1. 应向用户提供接受或拒绝的选项； 2. 用户选择接受或拒绝的操作应当一样简洁。为了不影响用户的选择自由，表达同意的机制应该与表达拒绝的机制具有相同的简洁水平和相同的技术方式。 3. 如果用户选择拒绝，不应遭受任何损害。用户表达的选择，无论是同意还是拒绝，都应以某种方式记录下来。 4. 界面不应使用潜在的误导性设计。	1）与其他各国相似，德国禁止“Cookie”墙； 2）德国监管机构未对《条款与条件》（Terms& Conditions)是否为有效的获取同意的方式进行明确表态，但大概率认为《条款与条件》不是有效的获取同意的方式，违反 GDPR 第 7（2）条。	1）不同意使用 Cookie 不应导致对网站内容访问的限制，也即禁止“Cookie 墙”。 2)用户必须能够以同样数量的行为（点击）在同样的层级接受或拒绝使用 Cookie，不论是针对全部的或是每个单独类别的 Cookie。	法国认为 Cookie 墙的使用应分情况讨论，英国虽态度负面，但依然持观望态度。 目前各国都强调，如果需要同意，用户必须在开始前给予明确、自由和明确的同意。
	同意的具	就使用 Cookie 征得用户同意必须与其他事项分	CNIL 强调，用户必须有机会针对每个单独的目的给予独立和具	与其他各国相似，德国要求向用户披	如果通过浏览器或其他应用程序设置获得同意，安	目前各国都强调，如果需要同意，用户必须在

	体性	开，因此不得以用户服务协议的方式征得用户同意。	体的同意。CNIL 指出，用户应该就特定目的给出特定的同意。就出于不同目的的不同的数据处理行为进行一揽子同意大概率是无效的。	露所有接收处理数据的对象。	装每一个 Cookie 都应请求数据主体的同意，而对数据主体预先通过浏览器或其他应用程序设置提供的所有 Cookie 的一般和抽象同意是无效的。	开始前给予明确、自由和明确的同意。
	同意的明确性	用户必须采取“明确且肯定的行动”来表示同意，用户继续浏览网站的行为不被视为其作出了有效同意，企业也不得使用任何预选框（或类似的符号，例如已经滑至特定位置的滑块）。	为了确保用户的同意是明确的，征得用户同意的机制必须确保使得用户充分了解收集其个人数据的目的和范围，不应使用可能存在误导性的设计。用户的同意应该是一个明确的、主动的动作（如点击 Cookie 横条上的“同意”）。 当追踪技术能够进行跨网站追踪时，每一个网站都应单独请求用户授权同意。	用户应明确表示同意。 虽然德国监管机构未就继续浏览网站是否构成同意进行明确解读，但根据实践，德国监管机构大概率也认为用户继续浏览网站并不等于该用户同意。	同意以用户明确积极的行为（clear positive action）为必要条件。因此，预先勾选、继续浏览或上下滚屏即视为同意的做法均不合法，由此产生的同意是无效的。 为保证用户不被网站设计（相对于选择拒绝，更有利于选择同意）所影响，接受或拒绝 Cookie 的按钮应使用同样的大小、基调和颜色。 不论选择同意或拒绝，存储用户选择的时间应为同样长度。	目前各国都强调，如果需要同意，用户必须在开始前给予明确、自由和明确的同意。 各国均强调，用户继续浏览网站并不等于该用户同意。
	同意的知	必须明确告知用户 Cookie	应当使用简明易懂的语言，充分	必须征得用户的同	必须征得用户的同意，并	目前各国都强调，如果

	情性	是什么以及 Cookie 在做什么，然后才能使用 Cookie 收集处理用户数据；若网站使用第三方 Cookie，则必须明确向用户告知第三方的身份，并说明第三方将如何处理 Cookie 数据。 如果网站设置了第三方 Cookie，网站和第三方都有责任确保用户清楚地了解 Cookie 使用情况并征得用户的同意。在这种情况下，网站必须确保其向用户告知了全面明确的信息，并确保用户对第三方 Cookie的使用享有接受或拒绝的权利。网站设置新的第三方 Cookie 时，需要重新征得用户同意。	告知用户使用各类追踪技术的目的。不得使用过于复杂的法律术语或技术术语。 在征得同意前，应向用户告知下列信息： 1) 收集使用 Cookie 方的身份； 2) 读写功能的作用与目的； 3) 用户进行同意及拒绝的路径； 4) 拒绝使用 Cookie 的后果； 5) 撤回同意的权利。 CNIL 同时建议企业提供详尽的数据控制者的清单以供用户参考，且该清单应定期更新。	意，并向其提供清晰、全面的 Cookie 使用信息。	向其提供清晰、全面的 Cookie 使用信息。	需要同意，用户必须在开始前给予明确、自由和明确的同意。且各国均要求，为了获得有效的知情同意，用户必须能够识别处理其数据的所有各方。这意味着应该列出所有依赖于用户同意的各方。
	同意的撤回和持续	企业应确保其设计的征得同意机制具有相应的技术能力，以允许用户以与做	用户应有权在任何时候撤回同意，且撤回同意应和做出同意一样易于操作。	用户必须能以做出同意相同的方式和可行性来撤销同	用户必须能以做出同意相同的方式和可行性来撤销同意。	各国的要求基本一致。

		出同意相同的简便程度撤回其同意。企业必须告知用户有关如何撤回同意以及如何删除已设置的Cookie的信息，例如在征得同意界面中说明或在隐私政策或 Cookie 政策中进行说明。 《ICO Cookie 指南》指出，用户选择接受或拒绝Cookie之后，企业不可频繁请求用户选择接受或拒绝。因此，企业应当根据在线服务的具体情况，确定合适的时间间隔，以再次向用户发送征求同意的请求。	建议企业确保允许用户撤回同意的选项应当在整个服务的过程中是易于获得的，获取的简便性可用所需花费的时间和访问撤回机制所需要的操作步骤数量进行衡量。	意。		
	获得同意的证明	N/A	CNIL 指出，根据GDPR第7条，同意应是可以证明的，企业应当建立相关机制用于证明其已经征得用户的有效同意。 CNIL 建议数据控制者能够提供以下证明：收集用户同意的证据；证明收集用户同意的机制是	N/A	N/A	N/A

			有效的(满足GDPR的同意标准)。CNIL 解释，可以使用如 CMP（Consent Management Platform）工具在满足此项要求。			
	Cookie 的保留期限	虽未规定 Cookie 保留期限的具体时间，但明确要求 Cookie 的保留期限必须与预期效果成比例，并且为达到目的所必须。	CNIL 建议将用户同意或拒绝的选择记录保存 6 个月。	没有具体制定。但德国认为较短的操作周期（也称为“可识别期”）更可能更满足 GDPR 利益平衡测试的要求 (GDPR6(1)(f))。	N/A	目前英国只规定了比例原则，但尚未规定 Cookie 的具体保留期限。法国针对收豁免的分析类 Cookie 规定了 13 个月的保留期限。
	Cookie banner 的实操建议	使用横条，弹出窗口，消息栏，标题栏或类似的消息框征得用户同意时，需要考虑其对用户体验的影响。例如，适用于台式机或笔记本电脑 Web 浏览器的消息框可能难以适用于移动设备（用户难以在使用移动设备时对该消息框进行阅读或与之交互）。	N/A	带有 Cookie 信息和一个简单的“确定”按钮是不够的。用户的同意必须是可识别的。这意味着 Cookie 弹窗必须详细列出所有需要同意的数据处理活动，并且用户必须能够拒绝这些选项。	《HDPA Cookie 指南》明确，下列行为是不合法的： 1）用户不选择接受 Cookie 即无法继续浏览。 2）仅在第二层级提供拒绝 Cookie 的选项。（如：在点击“更多信息”或“设置”的超链接后才出	N/A

		《ICO Cookie 指南》还强调，根据情况，预先选中非必要 Cookie 也有可能被视为“轻推行为”（nudge behaviour），即，影响用户做出特定行为，例如强调和突出接受选项，而淡化拒绝选项。这与 ICO《适龄设计规范》（Age Appropriate Design Code）的要求是一致的。			现拒绝 Cookie 的选项） 3）“同意”或“接受”按钮的大小和颜色设置诱导用户选择同意。如接受的选项更大，或以粗体显示，或已经提前勾选。 4）在用户同意或拒绝后，没有机会更改选择或只能通过浏览器设置更改选择。 5）在用户拒绝 Cookie 的情况下，通过弹窗频繁征求用户同意，而在做出同意的情况下，用户的选择被保存的时间更长。	
	通过浏览器征得同意	就目前的技术条件而言，依靠浏览器设置不能被视为征得用户有效同意的方式。	就目前的技术条件而言，依靠浏览器设置不能被视为征得用户有效同意的方式。	德国监管机构未就继续浏览网站是否构成同意进行明确解读，但根据实践，德国监管机构大概率也认为用户继续浏览网站并不等于该用户同意。	仅仅因为用户的浏览器配置接受 Cookie 不能被认为用户已经同意。	ICO 和 CNIL 的观点是，目前，仅仅依靠浏览器设置不足以获得有效的同意。德国数据监管机构与 HDPA 持相似意见。

环球律师事务所