合规指南

欧洲电信监管法规解读

推动车载互联服务加速落地

telenor IoT

目录

1. 概述

汽车行业正在经历一场前所未有的深刻变革。数字化服务正逐渐成为车辆的核心组成部分，重塑车辆的设计、营销和使用方式。如今，车载显示屏和应用程序已成为车辆的标准配置，驾乘者越来越期待能够流畅获享数字化内容，无论是工作、娱乐，还是通讯。

这些车载服务通常依赖车内集成的SIM卡来提供稳定的移动数据连接。通过车载信息娱乐系统实现流媒体播放、网页浏览和应用程序的使用。在此背景下，“车载互联服务”一词指的是人们在使用车辆过程中访问的数字化服务，获享这些服务需要移动数据支持。

尽管车主期望在驾驶过程中始终获得稳定且高质量的数字化服务体验，而汽车制造商也有意大规模提供此类服务，但在欧洲，法律框架却使这一目标变得困难重重。尤其是对那些希望打造合规且具备前瞻性的服务方案的企业而言，遵循各国的电信法规及相关法律框架是一项复杂的工作。

本白皮书聚焦这一核心挑战：欧洲推动跨境数字化服务发展的雄心，与汽车制造商及其合作伙伴在推出车载互联服务时所遭遇的监管碎片化之间存在冲突。具体而言，许多服务属于国家层面电信法规的管辖范围，而各国在法规解释和义务要求上的不一致，成为车载互联服务规模化发展面临的困境。

为了帮助车企应对这一复杂环境，本文将：

- 阐述提供车载数字化服务为何可能须履行《欧洲电子通信法典》(EECC)规定的义务
- 研究各国在SIM卡注册、合法拦截、数据留存及消费者权益法规方面的差异
- 分析法律要求影响服务设计、合规义务及产品上市时间的具体实践案例
- 为汽车制造商提供战略指导，应对复杂的监管环境。车企可自建服务或者与受监管的连接服务提供商(如Telenor IoT)合作。

本文基于Telenor IoT在全球30多个司法管辖区的运营经验，概述了汽车领域合作伙伴如何获益于Telenor在监管方面的专业知识和合规管理体系，同时仍能拥有对用户体验的自主控制权。对于汽车行业的决策者而言，本文旨在帮助他们应对欧洲复杂的监管环境，助其打造可扩展且合规的车载互联服务。本报告由Telenor IoT法规事务和汽车解决方案团队撰写，欧洲多国行业专家及法律专家对本报告亦有贡献。

2. 网联化愿景 vs 监管现状

联网服务正在重塑汽车工业。车载Wi-Fi、流媒体、实时导航和远程软件更新等功能不再只是可选配置，它们正在影响汽车的设计、营销和用户体验。[1]如今，车主期望数字化服务成为购车协议的一部分。对于汽车制造商而言，这些服务创造了新的收入来源，增强了品牌忠诚度，更能维系持久的客户关系。

这一切都源于车载互联服务。这些面向驾驶者和乘客的数字化服务依赖移动数据、稳定的网络连接，而且须符合车辆销售或使用所在国的合规要求。

然而，欧洲的监管环境为车载互联服务的顺畅、高效发展带来了一定挑战。尽管欧盟委员会支持跨境数字化服务发展，但各国的法规仍存在较大差异。移动网络运营商和汽车制造商在SIM卡注册、长期漫游、合法获取数据和用户知情同意等环节经常面临各国要求不一致的窘境。这些差异使得车载互联服务难以在整个欧洲范围内规模化推广。

2024年德拉吉（Draghi）关于欧洲竞争力的报告直接指出了这一问题。[2]报告警告称，监管碎片化正在损害欧洲的创新能力，同时呼吁各成员国制定更简化、更统一的规则，并敦促政策制定者消除阻碍跨境数字化服务发展的法律障碍。

与此同时，四大群体正在努力推动这一趋势的发展：

- **车主**希望获得无缝衔接的数字化服务，并愿意为此而更换品牌。[3]
- **汽车制造商**正在将软件和联网功能融入其产品核心战略。[4]
- **移动网络运营商**不再只是提供数据服务，而是成为企业在合规管理、系统整合和客户维护领域的合作伙伴。[5]
- **政策制定者**支持创新，但需出台能够推动规模化发展的明确的法律规定。

在接下来的篇幅中，我们将探讨欧洲车载互联服务所面临的监管障碍。但本文并不仅仅描述法律要求，而是结合实际运营经验，展示了这些法规对平台架构、服务接入、数据处理及合规管理等决策的影响。通过分享具体案例和面临的挑战，帮助决策者更深入地理解跨境服务落地过程中隐藏的复杂性，因为尽管从法律框架层面上看似清晰明了，但对于服务提供商而言，实际情况往往要复杂得多。

[1] 有关数字化服务如何改变竞争格局的更多信息，请参阅《非传统型合作伙伴关系：汽车制造商的制胜之道》，Telenor IoT Insights，2024年。点击查看
[2] 欧盟委员会（2024）德拉吉欧洲竞争力报告
[3] 麦肯锡（2024）《车联网：消费者的需求与付费意愿》
[4] 宝马集团（2025）《2024年年度报告》
[5] Telenor集团（2025）《2024年年度报告》

3. 一车多规：电信法规的多层级治理体系

欧洲的电信法规最初并非为网联汽车而设计。现行法律框架在传统的人与人通信和机器对机器（M2M）连接之间划定了清晰的界限。然而，现代车辆服务往往介于两者之间，将自动化系统与用户直接交互相结合。这种模糊性造成了一个监管灰色地带。

如今，大多数网联汽车都配有嵌入式SIM卡，支持互联网接入、OTA升级和车载娱乐等服务。其中一些功能，例如远程诊断可能属于M2M通信范畴，而另一些功能则明确涉及用户操作。如果驾驶者通过座舱系统播放音乐或浏览网页，则不能被归类为无人参与或有限人为干预的自动化数据交换。因此，此类使用场景可能不再符合典型的M2M通信范畴。由于这些服务面向广大终端用户，根据欧盟法律，它们更可能被归类为“公共电子通信服务”，这意味着服务商将承担更广泛和更严格的法律义务，尤其是在面向消费者时。

监管层面的复杂性自此开始显现。《欧洲电子通信法典》提供了核心的法律框架，但作为一项指令，它必须由每个成员国将其纳入本国法律加以实施。各国采取了不同的做法。一些监管机构关注终端用户是否积极主动地与服务进行交互；另一些则评估由谁提供连接技术，服务如何激活，或提供何种类型的内容。因此，相同的技术方案可能会因汽车的销售地或使用地不同而面临截然不同的监管处理方式。[6]

[6] Theißen, B., Lindner, D. (2022)《电子通信监管背景下的互联网接入服务》，ATZ Worldwide，第124期，50-53页。

这种不一致性带来的实际影响是，若车载互联服务被归入特定监管类别，则可能需遵守SIM卡注册、用户身份识别、合法拦截、数据留存及消费者保护等相关规定。正如欧洲电子通信监管机构（BEREC）所指出的，目前尚未形成统一的监管方法。[7]

对于构建跨境连接解决方案的企业而言，这种由各国规则拼合而成的监管格局带来了执行延迟、合规复杂性以及额外成本等问题。看似统一的欧盟框架，在实践中却存在显著差异。这种差异不仅影响合规管理，还影响产品设计、数据流管理和商业模式。

政策制定者已经意识到该问题。欧盟委员会的“数字十年”战略以及德拉吉竞争力报告[9]都呼吁，在统一市场建立更加清晰和一致的数字化服务规则。然而，相关进展仍然缓慢。在法律规定更明确之前，相关企业必须了解各国的法规，逐国应对复杂且碎片化的监管环境。

我们的观点

Telenor IoT认同欧洲监管机构目前的普遍解释，即车载互联服务属于适用扩展监管义务的监管范畴。此类服务提供商须履行《欧洲电子通信法典》及各国电信法所规定的相应义务。

然而，欧洲电子通信监管机构已明确指出，根据《开放互联网条例》，若所提供服务中包含车载Wi-Fi等，则必须被视为互联网接入服务。因此，它们必须遵守更广泛的要求，例如网络中立和透明义务。

我们也承认，相关议题目前仍处于积极讨论之中。欧洲电子通信监管机构指出，机器对机器通信与公共服务之间的界限并不总是泾渭分明。[10] 对《欧洲电子通信法典》的正式审查在法律上要求于2025年12月21日前完成，相关意见征询工作，包括关于《数字网络法案》（Digital Networks Act）的意见征集已经启动。[11] 这些进程可能有助于厘清面向消费者的物联网服务（包括车载互联服务）在欧盟境内的分类和监管方式。

3.1 授权机制：报备规则解析

对于服务提供商而言，首先要面对的监管环节之一是《欧洲电子通信法典》制定的通用授权框架。该框架旨在以更简化的报备机制取代个体许可，简化市场准入流程。然而，并非所有欧盟成员国都强制要求报备。各国自行决定是否需要进行报备，以及认定有效报备的具体要求。

例如，法国和丹麦并不要求向国家电信监管机构提交报备，而德国、西班牙和奥地利等国则要求在提供服务前必须完成报备。但这一区别常常被误解。许多人认为，如果无需报备，也就意味着无需履行其他电信相关义务。这种理解是错误的，《欧洲电子通信法典》适用于所有电子通信服务提供商，无论是否存在报备要求。消费者保护、数据安全以及与公共机构合作等要求，仍是所有服务商必须履行的义务。

[7] 欧洲电子通信监管机构关于通用授权制度在国家层面的实施与运行及其对内部市场运作影响之意见书——依据《欧洲电子通信法典》第122条第3款，2024年
[8] https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade
[9] 欧盟委员会（2024）德拉吉欧洲竞争力报告
[10] 欧洲电子通信监管机构报告：机器对机器通信与永久漫游（2024）
[11] 意见征询旨在收集利益相关方对特定问题的意见，但不一定导致立法变更；而审查作为正式程序，则可能导致法律框架的修订。

在要求报备的情况下，程序往往并不简单。欧盟委员会将其描述为“精简流程”，但欧洲电子通信监管机构在《关于通用授权的意见》中所揭示的现实情况是：各国在执行过程中存在碎片化、标准不一的问题，对于跨国经营的企业而言，往往带来不小的负担。[12]

“报备”一词听起来简单，但各国在实际操作步骤上存在显著差异，通常涉及大量的行政和法律工作。

根据我们的经验，常见的要求包括：

- 在国家级电信平台上注册，其中许多网站对英语的支持有限（例如奥地利、斯洛伐克和希腊）。
- 提交公司正式文件，例如公司注册证明或授权委托书，通常需要翻译、公证及认证。
- 授权代表身份核验，有时需提供护照或国民身份证的核证副本。
- 税务登记或本地税务识别号，例如克罗地亚的税务识别号（OIB），即使欧盟增值税指令规定成员国不得强制要求其他欧盟企业使用本国税务识别号。
- 无犯罪记录证明，捷克和丹麦要求提供。
- 格式要求不统一、指引不明确，报备流程从标准化的在线表格到非正式的电子邮件沟通，回复时间从即时批准到长时间无回应，差异显著。
- 需缴纳报备费。

这些例子表明，即使是一项看似简单的报备要求，也可能存在碎片化执行细则，导致企业资源耗费，对于希望快速且合规地布局整个欧洲市场的服务提供商而言尤其如此。

我们的观点

对汽车制造商的影响

对于汽车制造商而言，这些法规的差异不仅仅是法律细节，它们直接影响到数字化服务在新市场中落地的速度和可靠性。汽车制造商应与具备通用授权制度实践经验、且能清晰阐明其合规框架构建方式的移动网络运营商合作。借助运营商已有的合规管理经验，可以显著缩短产品上市周期，规避意外的法律和财务风险。

当汽车制造商考虑自行注册为服务提供商时，应意识到这一过程可能比表面看起来更加复杂且耗时。每项报备都必须符合各国特定的法规要求，而初期准备往往涉及法务、技术和合规团队之间的协作，远非填写一份表格那么简单。

[12] 欧洲电子通信监管机构关于通用授权制度在国家层面的实施与运行及其对内部市场运作影响之意见书——依据《欧洲电子通信法典》第122条第3款，2024年

3.2 数据留存挑战

数据留存是最为复杂和敏感的法律义务之一。其核心要求是存储用户及其通信会话的特定元数据，以便执法部门能够依法访问这些数据。

虽然欧洲法院已裁定，不允许进行普遍且无差别的数据留存，但各成员国仍可在特定条件下规定本国的数据留存义务。由此形成了碎片化且快速变化的监管环境，给跨国运营的服务提供商带来了重大的合规管理挑战。[13]

数据留存的复杂性首先体现在可能需要保留的数据类型上。

这通常包括：

- 用户数据，用于识别服务使用者的信息
- 通信数据，例如源IP地址和目的IP地址及时间戳
- 位置数据，设备在特定时间点的位置信息

每个国家对这些类别有不同的定义，并自行制定数据存储期限规则。在一些欧盟成员国，法律并未规定必须保留任何数据；而在其它成员国，服务提供商被要求存储特定的数据集，留存期限因数据类型而异。[14]

例如：

- 在意大利，计费相关通信数据必须保留6个月，而位置数据则必须保留12个月。
- 在爱尔兰，仅需留存极少类型的通信数据。
- 在罗马尼亚，须保留更多类型的用户数据和通信数据，最长留存期限可达3年。

这些差异不仅体现在法律层面，它们会对系统设计产生直接影响，要求服务提供商针对每个司法管辖区调整数据存储、安全和访问控制流程。某些情况下，可能需要具备本地访问数据能力、配置独立的留存界面，或保留特定国家的用户同意机制。若未能遵守数据留存和保护义务可能会导致严重的法律后果，包括声誉受损、监管调查以及依据该国或欧盟法律面临高额罚款。

3.2.1 通信数据留存：各国法规差异显著

在所有留存数据类型中，通信数据是最缺乏统一监管的类型之一。核心问题在于服务提供商是否必须保留通信目的地的信息，例如用户访问的网站。

德国和比利时等国规定，除非满足特定法律条件，否则禁止存储目的地数据；而波兰和罗马尼亚等国则强制要求留存此类数据。

即使在同一国家，留存期限也可能因数据类型不同而存在差异。一些国家可能要求服务提供商保留通话元数据6个月，而位置数据则需保留12个月。这使得在不同国家之间建立统一的数据留存架构变得十分困难。

[13] 高级别小组总结报告：数据获取以促进有效执法（2024）
[14] 欧洲刑警组织（2024）SIRIUS项目：欧盟电子证据现状报告

3.2.2 用户身份核验

数据留存经常与用户身份核验相混淆，但两者是不同的法律义务。一些成员国要求进行SIM卡注册，这意味着服务提供商必须通过有效的护照或国民身份证来收集并核验用户身份。

奥地利的规定更为严格，要求每一张SIM卡，包括预付费卡或机器对机器通信订阅卡，都必须与经过验证的用户身份绑定。[15]虽然用户身份验证不属于数据留存义务的范畴，但直接影响留存数据对执法部门的有效性。如果允许匿名或使用化名，就更难将一次通信会话与特定个人关联起来。

需要着重指出的是，现行多数核验法规均针对传统手机用户设计，并不适用于车联网场景，在此类场景中，移动通信服务的订阅主体通常是汽车制造商、租赁供应商或经销商，而非实际使用人。

有鉴于此，一些监管机构提出了替代机制。比利时邮政和电信管理局BIPT和英国的通信管理局（Ofcom）都指出，将SIM卡与车辆识别码（VIN）关联起来是一种有效的追溯机制。这使得执法部门能够将SIM卡的使用情况与国家车辆数据库进行交叉比对。这是一个切实可行的解决方案，尤其适用于车辆最终用户可能频繁变更的场景。

3.3 合法获取数据与拦截

如果您的车辆集成了流媒体、游戏平台或语音助手等网联服务，这些服务可能会被归类为公共电子通信服务，因此需要承担电信监管义务，包括支持合法获取数据的要求。合法获取数据指执法部门依法获取所需的用户信息或通信会话数据。虽然此类要求通常由您的网络连接合作伙伴来处理，但相关责任及声誉风险仍可能对您的品牌造成影响。

用户身份验证和数据留存的目的相同：支持合法获取数据。警方或情报机构在调查过程中可依法调取数据。尽管欧盟法律提供了总体框架，但各成员国在实施细则上存在很大差异。[16]

一些国家要求部署实时拦截系统，另一些国家则允许在接到请求后进行安全的数据移交。根据欧盟《电子证据条例》，从2026年8月起，欧盟成员国执法机关可直接向其他成员国的服务提供商发送获取电子证据的指令。此举虽旨在简化执法流程，但服务提供商必须在其运营的每个国家做好准备，及时响应指令要求。

当前，统一监管框架的缺失正引发严峻挑战。最近的一项研究指出，现行政策存在相互重叠甚至相互矛盾的义务条款，导致服务提供商不确定应适用哪些规则或面对相互冲突的要求时无所适从。

[15] Rundfunk und Regulierungs-GmbH (2025)。所有预付费电话卡必须登记。
[16] Doronin V. (2023)《合法拦截 —— 欧盟的市场准入壁垒》，《计算机法律与安全评论》，第51卷（2023年）105867

甚至像“有效请求”或“必需数据”这样的基本术语，各国的解释也不尽相同。这对于布局整个欧洲市场的服务提供商而言，造成了法律上的不确定性及执行层面的延宕。

许多服务提供商低估了数据调取量。在2020年至2022年期间，欧盟执法机构发出了超过172,000次跨境数据调取请求。[17]

最常见的数据调取涉及以下内容：

- IP地址使用情况
- 用户身份信息
- 登录时间
- 位置数据

仅在2022年，就有超过4,500次紧急数据调取请求，通常要求在24小时之内做出回应。[18]

因此，服务提供商需要有明确的内部作业流程来处理以下事项：

- 接收和验证请求
- 提取正确的数据
- 记录所共享的信息
- 安全传输数据

这些不仅仅是法律程序问题，它们还影响到团队职责、系统架构以及车企与连接服务提供商之间的协作方式。如果没有明确的职责划分和对当地市场、法规等的深入理解，几乎不可能以合法、合规且可扩展的方式实现数据访问。

我们的观点

对汽车制造商的影响

从技术和监管的角度来看，合法获取数据相关事宜通常是由移动网络运营商负责。然而，对于集成联网服务的汽车制造商而言，不合规带来的后果可能远远超出网络使用层面。商誉风险、服务中断以及违规的数据流都可能影响终端用户体验以及车企的品牌形象。

因此，汽车制造商应确保其连接服务合作伙伴不仅在理论上，更要在实践中履行法定监管义务并且有完善的运作流程，包括齐备的书面流程和上报机制，以及在运营国法律或欧盟《电子证据条例》规定的时限内做出响应的能力。

对于计划直接提供连接服务的汽车制造商而言，无论是通过提供品牌化服务，还是直接与客户签订合约，合规门槛都将大幅提高。在这些情况下，汽车制造商自身可能需要承担依法提供数据的义务。他们必须能够验证数据调取方的身份、提取有效数据，并确保信息披露合法、安全且有规范的档案记录。

合法获取数据已不再是一个边缘化的技术问题，而是一个需要跨部门协作的合规挑战。正确应对这一问题，不仅对满足监管要求至关重要，更关系到用户对联网服务的信任度。

[17 & 18] 欧洲刑警组织（2024）：SIRIUS项目报告

4. 车载互联场景中的消费者权益保护义务

除了注册和数据法规外，提供车载互联服务还须履行《欧洲电子通信法典》中规定的一系列消费者权益保护义务。虽然这些规定在传统的电信服务领域已经日臻完善，但应用在车联网领域，尤其是当服务已内嵌集成且用户无显性成本时，往往颇具挑战性。

如果汽车制造商或其合作伙伴被归类为受监管的服务提供商，则通常需遵守以下规则：

- 清晰易懂且便于获取的合同（EECC第102条）：服务提供商必须以可持久保存的载体形式向客户提供合同，所有条款须以易于理解的方式呈现。
- 标准化合同摘要（EECC第102条第3款）：在达成协议前，必须提供一份欧盟通用的合同摘要。
- 网速和服务质量的透明度义务（EECC第103条）：服务商必须披露典型上行/下行网速数据，并明确发生网速偏差情况时的具体处理机制。
- 投诉处理义务（EECC第104条）：服务提供商必须提供用户友好的投诉流程，并设定明确的响应时限。
- 简化更换运营商流程（EECC第106条）：如果允许用户自主更换SIM卡或切换通信服务提供商，则需保障用户享有服务连续性和号码携带等相关权利。
- 捆绑服务与合同期限规则（EECC第105条和107条）：若连接服务属于整车服务的一部分，则对合约锁定期限和续签的限制条款也适用相关规定。

这些规则并非抽象的概念。如果汽车制造商被认定为服务提供商，则须承担《欧洲电子通信法典》规定的全部消费者权益保护义务，[19] 而这些义务通常并未纳入车企现有运营模式中。欧盟各国对这些规则的解释和执行方式各不相同。在五个成员国推出的同一项服务，可能需要准备五套不同的文件、五种语言版本，并遵循五套不同的流程。

我们的观点

汽车制造商应与连接服务提供商紧密合作，明确职责划分。作为受监管服务提供商，Telenor IoT全权承担消费者权益保护合规义务，包括相关文件的准备、各国实施差异的应对以及与监管机构的沟通等环节。如果车企考虑自主提供该服务，则应在部署前完成全面法律评估。预先规划消费者权益保护合规工作，有助于车企降低风险、避免项目延误，并确保在所有目标市场中以合法合规的方式提供一致的用户体验。

[19] 汽车制造商可能会主张，联网服务作为整体车载数字体验的一部分，应归为附属服务，因此适用更宽松的监管制度。为贴合实际，本白皮书不再进一步探讨这一法律细节。

5. 规模化车载互联服务部署亟需核心环节清晰透明

打造欧洲全境品牌化、规模化的无缝车联网数字体验的目标宏大而清晰。但合规之路并非一蹴而就。从Wi-Fi热点到流媒体，每一项功能都会牵涉一系列法律义务。这些义务因国家而异、随时间变化且往往反映出对互联网服务交付方式的认知有待更新。

本文仅简要介绍了这些挑战的其中一部分，重点探讨了授权机制、数据留存、用户身份核验、合法获取数据以及消费者权益保护等内容。上述每一个环节都可能需要数月的法律分析和跨部门协调，而这些还只是诸多挑战的冰山一角。编号资源、增值税处理、紧急呼叫合规性以及频谱使用等问题的复杂程度不相上下，目前许多欧盟成员国正就此展开积极讨论。

然而，如果从一开始就将合规管理融入服务设计体系，这些难题可以迎刃而解。与Telenor IoT携手，汽车制造商在保留用户体验自主控制权的同时，将监管合规和运营责任转移给我们。作为汽车行业值得信赖的连接合作伙伴，我们凭借数十年的经验、成熟的全球网络，以及在合规管理和大规模部署方面的深厚专业知识为客户提供支持。

我们的解决方案设计简洁明了，性能出众：

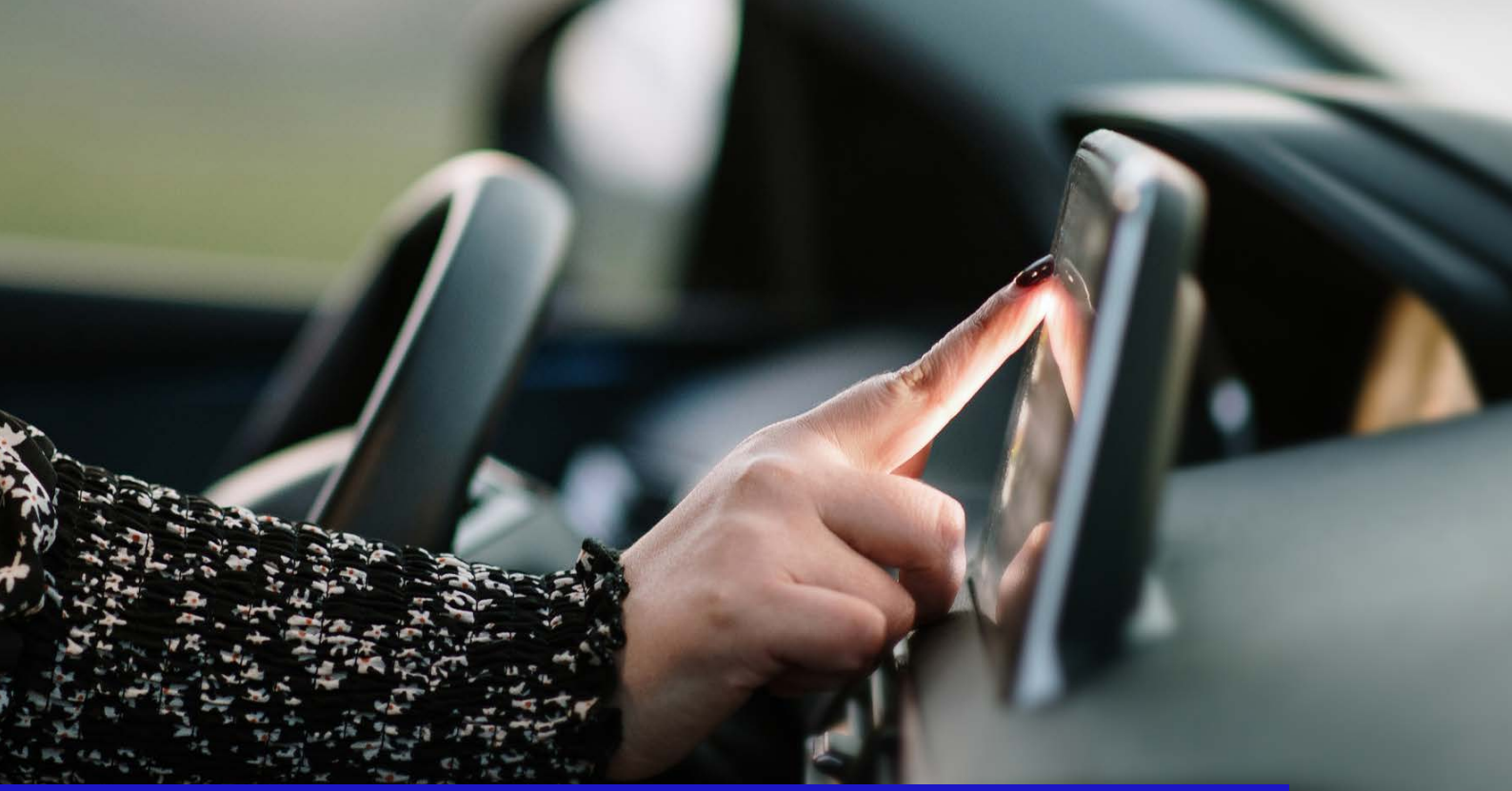
- 汽车制造商始终自主掌控品牌、用户流程和服务方案，通过API实现与现有生态系统的无缝整合。
- Telenor IoT提供合规运营的互联网服务 —— 全面负责合规管理、消费者权益保护、合法调取数据及数据处理。
- 方案架构具备弹性扩展能力 —— 全面符合各国电信法规、《欧洲电子通信法典》以及欧洲监管机构的合规要求。

欢迎与我们联系

无论您所在企业处于市场启动筹备期、合规风险评估期，还是新服务模式探索期，我们随时为您提供支持。我们的团队深谙欧洲电信与数据法规脉络，能够协助您设计出兼具合规性与前瞻性的解决方案。

欢迎与我们联系，在保障用户体验和品牌自主权的前提下，为您的车联网战略奠定坚实的法律基础。

✉ hello@telenorconnexion.com



6. IoT Drive: 开启汽车智能连接新篇章

20余年来，Telenor IoT持续推动车联网技术发展，服务全球数以百万计的车辆。在此基础上，我们如今正致力于汽车行业转型的新阶段：车辆正逐步演进为个性化数字服务平台。

我们于2024年推出了Consumer Connect（车主连接平台）。作为IoT Drive解决方案的组成部分，Consumer Connect基于我们的管理连接服务构建，既能助力汽车制造商满足合规要求，支持创新的商业模式，又能提供无缝用户体验。

在当今的软件定义汽车时代，从远程信息处理、紧急呼叫系统（eCall），到OTA升级、高级驾驶辅助系统、信息娱乐系统及能源管理，每一项功能都依赖安全、持续的网络连接。网络连接已成为汽车行业提升核心竞争力的基石。

然而，车辆联网所带来的合规监管和技术上的挑战远超常规物联网范畴。Consumer Connect直面这些挑战，助力车企实现合规运营、服务变现，并为用户提供流畅的数字化体验。

核心功能

- 数据付费双轨机制：车企付费与终端用户付费两种模式
- 基于API集成方案：支持整车厂提供品牌化用户体验
- 本地IP地址分配：根据驾驶者所在国家或地区分配本地IP，实现本地化服务
- 终端用户身份验证与授权管理：流程高效且安全
- 合规事务合作伙伴：Telenor IoT作为终端用户的互联网服务提供商，确保符合监管要求

凭借全球化布局和数十年的专业积淀，Telenor IoT提供规模化的无缝连接服务，助力汽车制造商加快产品上市、在全球市场保持合规，并提供当今驾乘者所期望的可靠数字化服务。

telenor IoT

关于Telenor IoT

Telenor IoT是全球知名电信运营商Telenor集团旗下的物联网业务品牌，提供物联网综合解决方案。作为全球领先的物联网解决方案提供商之一，20多年来，Telenor为各种规模的企业提供全球物联网连接服务、云服务和专业支持。

Telenor IoT在约200个国家和地区为客户管理逾2,500万台联网设备，服务于沃尔沃、斯堪尼亚、日立、Verisure Securitas Direct和富世华等全球化企业。

我们在北欧经由Telenor在当地的机构提供物联网解决方案，在全球其他地区则由Telenor Connexion为需要定制产品和服务以及专业支持的大型跨国企业提供物联网解决方案。

iot.telenor.com　　hello@telenorconnexion.com