数据保护官沙龙（DPO Salon）公益出品

EDPB 车联网个人数据保护指南

（中译文）

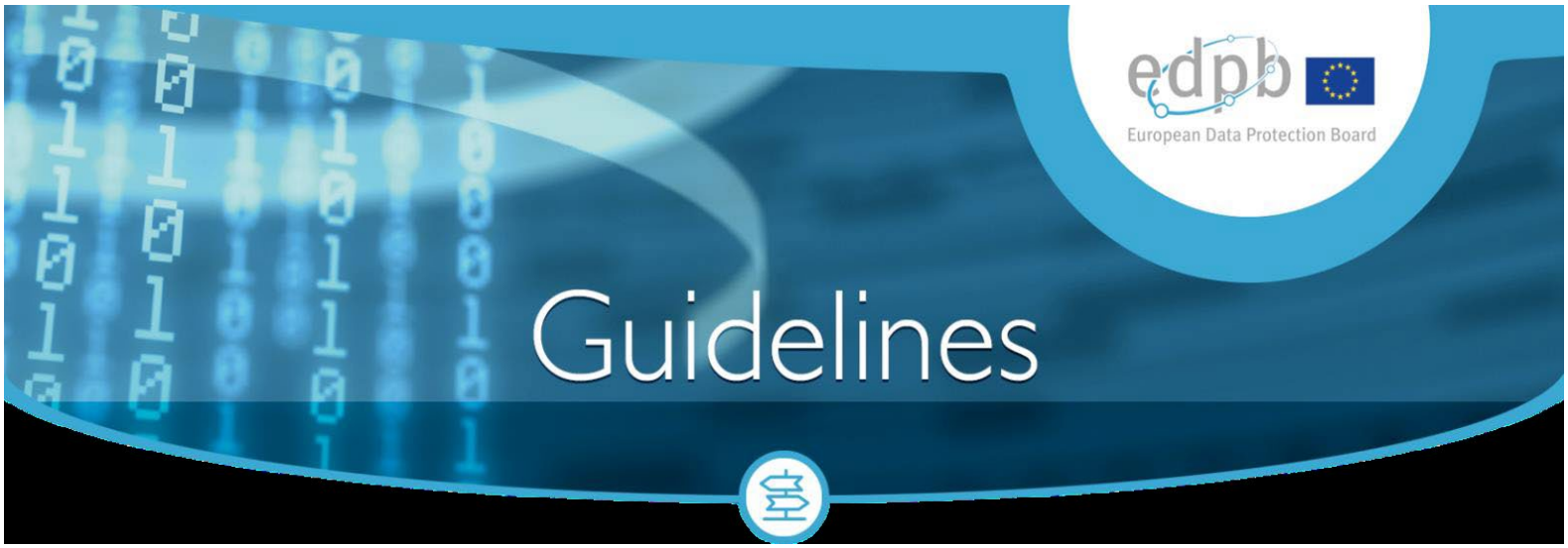
译者（姓氏音序排名）：

刘文丽、王晶晶、余扬横波

审校：

何姗姗、罗为、王新锐

2020 年 3 月



在联网车辆和出行相关应用环境下处理个人数据的指南

（车联网个人数据保护指南）

第一版

2020 年 1 月 28 日通过

目录

欧洲数据保护委员会（EDPB）

根据欧洲议会和欧洲理事会 2016 年 4 月 27 日发布的《关于保护自然人的个人数据处理和数据的自由流动、废止第 95/46/EC 号指令的第 2016/679/EU 号条例》（以下简称“GDPR”）第 70 条第 1 款 e 项，

根据《欧洲经济区协议》，特别是其附录 XI 和第 37 号协议，其经欧洲经济区联合委员会 2018 年 7 月 6 日第 154/2018 号决定修改 [1]

根据其《议事规则》第 12 条和第 22 条，

通过以下指南：

1. 序言

作为 20 世纪经济的象征，汽车是影响了整个社会的大众消费品之一。汽车通常与自由的概念联系在一起，其往往不仅仅被视作一种交通工具。实际上，它们代表了一种私人领域，人们可以在其中享受到一种决定自主权，并且免受任何外部干扰。今天，随着联网车辆进入主流，这样的一种看法与现实不再相符了。车载网络连接迅速从豪华车型和高档品牌拓展到大量的中端车型，汽车正在成为巨大的数据枢纽。不仅仅是车辆，驾驶员和乘客也变得越来越互联了。事实上，过去几年内上市的许多车型都搭载了传感器和车载网联设备，他们可能会收集和记录发动机性能、驾驶习惯、逗留过的地点，甚至是驾驶员的眼睛动作、脉搏或其他用于身份认证或识别的生物识别数据以及其他数据。[2]

这种数据处理发生在一个复杂的生态系统中，参与者不限于汽车行业的传统玩家，属于数字经济的新兴玩家也参与了对这一生态系统的塑造。这些新兴玩家

[1] References to “Member States” made throughout this document should be understood as references to “EEA Member States”.
[2] Infographic “Data and the connected car” by the Future of Privacy Forum; https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf

可能提供信息娱乐服务，诸如在线音乐、路况和交通信息，或者提供驾驶辅助系统和服务，例如自动辅助驾驶（autopilot）软件、车况更新、基于驾驶行为的保险（usage based insuarance）或动态地图绘制。此外，由于车辆通过电子通信网络实现互联，参与这一过程的道路基础设施管理者和电信运营商在对驾驶员和乘客的个人数据的潜在处理操作中也发挥着重要的作用。

除此之外，联网车辆产生越来越多的数据，其中多数都可被视为个人数据，因为它们会关联到驾驶员或乘客。即使一辆联网汽车不直接关联到一个人名，但是从技术方面和车辆特征上，它会关系到汽车的驾驶员或乘客。例如，驾驶风格或行驶里程相关的数据、车辆零部件磨损的相关数据或摄像头收集的数据可能涉及驾驶员行为以及车内或车外其他人的信息。

2016 年，国际汽车联合会（FIA）在欧洲开展了一项叫做“我的汽车我的数据”的活动，以了解欧洲人对联网汽车的看法。[3]该活动显示出驾驶员对互联性有很大兴趣的同时，它也强调了在使用车辆产生的数据时必须提起警惕和遵守个人数据保护法律是十分重要的。因此，挑战在于，对于每一个利益相关者来说，都要从产品设计阶段就要融入“保护个人数据”的维度，确保汽车使用者在其数据上享有透明度和控制。这样一种方式可以帮助增强用户的信心，从而促进这些技术的长期发展。

1.1 相关工作

在过去的十年间，联网车辆已经成为监管者的重要课题，特别是最近几年有大幅上升。国家和国际层面都发布了很多关于联网车辆安全和隐私的文件。这些法规和倡议旨在用特殊行业规则补充现有的数据保护和隐私框架，或为专业人员提供指导。

1.1.1 欧洲和国际层面法案

自 2018 年 3 月 31 日起，所有 M1 和 N1 新车（乘用车和轻型车）都必须强

[3] Campaign “My Car My Data”; http://www.mycarmydata.eu/

制安装基于 112 的车内自动紧急呼叫（eCall）系统。[4, 5] 2006 年，欧盟第 29 条工作组（WP29）通过了一项关于 eCall 法案中的数据保护和隐私影响的工作文件。[6]此外，正如此前所讨论的，第 29 条工作组在 2017 年 10 月也通过了一项关于在协同智能交通系统（C-ITS）环境下处理个人数据的意见。

2017 年 1 月，欧盟网络和信息安全局（ENISA）发布了一份聚焦于智能汽车网络安全和恢复力的研究，列举了敏感资产以及相应的威胁、风险、消减因素和可能实施的安全措施。[7]2017 年 9 月，数据保护与隐私专员国际大会（ICDPPC）通过了一项关于联网车辆的决议。[8]最后，在 2018 年 4 月，国际通信数据保护工作组（IWGDPT）也通过了一项关于联网车辆的工作文件。[9]

1.1.2 EDPB 成员国法案

2016 年 1 月，德国联邦和州独立数据保护机构会议和德国汽车工业协会（VDA）就联网和非联网车辆的数据保护原则发布了一份共同声明。[10]2017 年 8 月，英国联网和自动驾驶汽车中心（CCAV）发布了一项指南，陈述联网和自动驾驶汽车的网络安全原则，旨在提高汽车行业对此问题的意识。[11]2017 年 10 月，法国数据保护机构——国家信息与自由委员会（CNIL）发布了联网汽车的合规一揽子建议，为利益相关者在如何集成设计和默认的数据保护方面提供协助，使数据主体能够有效控制他们的数据。[12]

---

[4] The interoperable EU-wide eCall; https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en
[5] Decision No 585/2014/EU of the European Parliament and of the Council of 15 May 2014 on the deployment of the interoperable EU-wide eCall service Text with EEA relevance; https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32014D0585
[6] Working document on data protection and privacy implications in eCall initiative; http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf
[7] Cyber security and resilience of smart cars; https://www.enisa.europa.eu/publications/cyber-security-andresilience-of-smart-cars
[8] Resolution on data protection in automated and connected vehicles; https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connectedvehicles_en_1.pdf
[9] Working paper on connected vehicles; https://www.datenschutz-berlin.de/infothek-undservice/veroeffentlichungen/working-paper/
[10] Data protection aspects of using connected and non-connected vehicles; https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf
[11] Principles of cyber security for connected and automated vehicles; https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles
[12] Compliance package for a responsible use of data in connected cars; https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data

1.2 适用法律

与此相关的欧盟法律框架为《通用数据保护条例》。联网车辆下任何涉及处理个人数据的数据处理情形均适用该条例。

除 GDPR 外，《电子隐私指令》（第 2002/58/EC 号指令，经第 2009/136/EC 号指令修改）**为欧洲经济区内所有想要存储或访问订阅者或用户存储在终端设备中的信息的参与者设定了特别标准。**

实际上，如果说大多数《电子隐私指令》的条款（第 6 条、第 9 条等）适用于公共电子通信服务的提供商和公共通信网络提供商。《电子隐私指令》的第 5 条第 3 款则是一个通用条款。它不仅适用于电子通信服务，还适用于存放或读取终端设备的信息而不考虑存储或访问的数据的性质的所有实体。

至于“终端设备”的概念，其定义规定在第 2008/63/CE 号指令中。第 1（a）条定义终端设备为一个“直接或间接与一个公共电线网络的接口相连接，从而发送、处理或接收信息的设备；在任一情形下（直接或间接），连接可通过电线、光纤或电磁的形成完成；若设备被放置在终端和网络接口中间，连接是间接的；（b）卫星地球站设备”。

因此，联网车辆和任何一个与其相连的设备均会被视为一个“终端设备”（就像一台电脑，一部手机或一台智能电视），《电子隐私指令》第 5 条第 3 款在相关情形下必须适用。

正如近期 EDPB 在其《5/2019 关于<电子隐私指令>和 GDPR 相互作用的意见》中所概述的那样 [13]，《电子隐私指令》第 5 条第 3 款规定，一般来说，在一个订阅者或用户的终端设备中存储信息、访问已经存储的信息必须取得事先同意。就存储在终端用户的设备中构成个人数据的信息而言，在存储或访问信息的活动方面，《电子隐私指令》第 5 条第 3 款优先于 GDPR 第 6 条适用。[14]任何在前述

[13] European Data Protection Board, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019, paragraph 40.
[14] Ibid, paragraph 40.

处理操作后进行的个人数据处理操作，包括处理通过访问终端设备的信息而获得的个人数据，必须另外具备 GDPR 第 6 条下的某一法律依据，才能保证其合法性。[15]

当遵守《电子隐私指令》第 5 条第 3 款的规定寻求存储或访问信息的同意时，数据控制者必须告知数据主体其全部处理（包括在前述操作后的任何处理）的目的，此时的同意通常能涵盖这种处理操作。同意可能构成存储、访问已经存储的信息，以及在前述处理操作后进行的个人数据处理的法律依据。实际上，当评估是否符合 GDPR 第六条时，应当考虑到，从整体而言，处理包括那些欧盟立法机关寻求为其提供额外保护的特定活动。[16]此外，数据控制者在确定适当的合法性依据时必须考虑对数据主体权利的影响，以遵守公平原则。[17]底线是，数据控制者不能依据 GDPR 第 6 条来降低《电子隐私指令》第 5 条第 3 款所提供的额外保护。

EDPB 回顾说，《电子隐私指令》中同意的概念保留其在 GDPR 中的概念，必须满足 GDPR 第 4 条第 11 款和第 7 条规定的同意的全部条件。

然而，如果同意是原则，《电子隐私指令》第 5 条第 3 款允许存储信息或访问已经存储在终端设备中的信息可以豁免告知同意的要求，如果其满足以下条件之一：

- 豁免 1：仅为完成通信在电子通信网络上的传输之目的；
- 豁免 2：当该信息对于信息社会服务的提供商提供订阅者或用户明确要求的服务来说是绝对必要时。

在该类情形下，处理个人数据，包括通过访问终端设备中的信息而获得的个人数据，是基于 GDPR 第 6 条规定的法律依据之一而进行的。

---

[15] Ibid, paragraph 41.
[16] Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, paragraph 41.
[17] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, paragraph 1.

1.3 范围

本文件尤其关注与数据主体对联网车辆的非专业使用相关的个人数据处理，这些数据主体包括例如驾驶员、乘客、车主、承租人等。更具体地说，本文件关注（1）在车内处理的个人数据，（2）车辆和与之相连接的设备（如用户的智能手机）之间交换的个人数据，或（3）在车内收集和为进一步处理而向外部实体（如汽车制造商、基础设施管理者、保险公司、汽车修理者）输出的个人数据。

在本文件中，联网车辆的定义应当按照一个广义的概念来理解。它可以被定义为一辆装配有许多电子控制单元（ECU）的车辆，这些电子控制单元通过车内网络以及网联设施连接在一起，网联设施使其能够与车内和车外的其他设备分享信息。如此，数据可以在汽车和与之相连的个人设备间进行交换，比如允许手机应用镜像到汽车的仪表盘信息和娱乐单元。同样的，独立的手机应用的开发，即车辆在协助驾驶员时是非独立的（例如，依赖于智能手机的唯一使用），也被包括在本文件的范围内，因为它们也帮助提高了车联的网联能力，即使它们可能不能有效地依赖于与车辆自身的数据传输。联网车辆的应用多种多样，可能包括[18]：

*出行管理：*使得驾驶员可以迅速、经济高效地到达目的地的功能，通过提供及时的 GPS 导航、潜在危险环境情况（如道路结冰）、交通拥堵或道路施工、停车场或车库辅助、优化的油耗或道路收费相关的信息。

*车辆管理：*帮助驾驶员减少运行成本、提升简便操作的功能，例如车辆状况通知和服务提醒、使用行为数据的传输（比如为车辆修理服务之目的）、定制化的现驾现付型（Pay As/How You Drive）保险、远程操作（例如供暖系统）或概要配置（例如座椅位置）。

*道路安全：*提醒驾驶员外部危险和内部响应的功能，例如碰撞保护、危险警告、车道偏离警告、驾驶员疲劳检测，紧急呼叫（eCall）或交通事故调查“黑匣子”（事件数据记录器）。

[18] PwC Strategy 2014. “In the fast lane. The bright future of connected cars”; https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf

*娱乐：*为驾驶员和乘客提供信息和娱乐的功能，例如智能手机界面（脱手电话、语音生成文本消息）、WLAN 热点、音乐、视频、互联网、社交媒体、移动办公或“智能家居”服务。

*驾驶员辅助：*部分或全部自动驾驶的功能，例如交通拥挤、泊车或高速场景下的运行协助或自动辅助驾驶。

*健康：*监测驾驶员驾驶舒适度、能力和健康状况的功能，例如疲劳检测或医疗救助。

因此，车辆本身可能是联网或非联网的，个人数据可以通过若干方式收集，包括：（1）车辆传感器，（2）车载 T-BOX（telematics box），或者（3）手机应用（例如通过属于驾驶员的设备来收集）。如落入本文件范围，手机应用需与驾驶环境相关。例如，GPS 导航应用确实属于本文件范围，但为用户推荐兴趣点（餐厅、历史古迹等）的应用不属于本文件涵盖范围。

由一辆联网车辆产生的大多数数据与以识别或可识别的自然人相关，因此构成个人数据。例如，数据包括直接可识别的数据（比如驾驶员的完整身份），以及间接可识别数据，例如行驶旅程的细节、车辆使用行为数据（比如与驾驶风格相关的数据或行驶里程）或者车辆的技术数据（例如车辆零部件磨损有关的数据），这些数据通过与其他资料相互对照，特别是与车辆识别号（VIN）相对照，可以关联到自然人。联网车联的个人数据也可能包括元数据，例如车辆保养状况。也就是说，任何可以与一个自然人相关联的数据都会落入本文件的范围。

联网车辆生态系涵盖了大范围的利益相关者。更确切的说，它包括了汽车行业的传统参与者以及来自数字行业的新兴玩家。

因此，本指南针对汽车制造商、设备制造商和汽车零部件供应商、汽车维修商、汽车经销商、汽车服务提供商、租赁和共享汽车公司，车队管理商、机动车保险公司、娱乐提供商、电信运营商、道路基础设施管理方和公共部门以及驾驶员、所有人、承租人和乘客。上述为不完全列举。

1.3.1 非本文件范围

为其雇员提供公司车辆的雇主可能想监控其雇员的行动（例如为确保雇员、货物或车辆的安全，为分配资源，为追踪和为一项服务开账单或者为了检查工作时间）。在此背景下雇主所实施的数据处理引发了雇佣语境的特别考虑，这可能是由国家层面的劳动法所规定，因此无法在本文的指南中进行详细说明。

联网车辆无线电感应系统，它们受到诸如 WiFi 或蓝牙追踪等被动追踪。在此意义上它们与其他联网设备并无不同，并且落入《电子隐私指令》的范围，《电子隐私指令》目前正在被修订。本文因此也不包括由使用普通智能手机位置服务的旁观者构成的密集网络对配备 WiFi 的车辆 [19]的大规模追踪。这种服务例行向中央服务器报告所有可见的 WiFi 网络。由于内置 WiFi 可被视为一个二级车辆识别符 [20]，它承受着在第三国被系统性、持续收集完整车辆活动资料的风险。

车辆越来越多地配备了图像记录装置（例如停车摄像头系统或车内摄像头）。由于这涉及对公共场所进行拍摄的问题，需要对相关的立法框架进行评估，而这是特定于每个成员国的问题，因此该种数据处理也不在本文件的范围。

促使协同智能驾驶系统（C-ITS）运行的数据的处理活动——如在欧盟《第 2010/40/EU 号指令》[21]中规定的那样，第 29 条工作组已经在一项特别意见 [22]中进行了论述。通过该意见，第 29 条工作组聚焦于为初始部署所建立的特别用例，致力于在后期评估那些当实施更高等级的自动化时一定会出现的新问题。由于 C-ITS 环境下数据保护的影响十分特定（空前大的位置数据量、个人数据的持续广播、车辆和其他道路基础设施的数据交互等），欧盟层面正在讨论当中，因此，该种环境下的数据处理不在本文件的范围之内。

最后，本文件并非旨在解决联网车辆可能带来的全部问题，因此不应被视为

[19] See https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html for details

[20] Markus Ullmann, Tobias Franz, and Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier -- Analysis, and Measurements, in Proceedings, VEHICULAR 2017, The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nice, France, July 23 to 27, 2017, pages 32 to 37.

[21] Directive on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0040

[22] WP29 - Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS); http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171

详尽无遗。

1.4 定义

处理：个人数据的处理包括涉及个人数据的任何操作，例如收集、记录、整理、结构化、存储、调整或改变、恢复、咨询、使用、通过传输披露、分发或提供、对齐或组合、限制、删除或销毁等。

数据主体：指与处理行为所涉及的数据相关的自然人。在联网车辆的语境下，它尤其可能是驾驶员（主要或偶尔）、乘客或车辆的所有人。

数据控制者：指决定发生在联网车辆中的处理行为的目的和方式的人。数据控制者可能包括处理车辆数据以向驾驶员发送交通信息、环保驾驶消息或就车辆运行状况发送警示的服务提供商、提供“现驾现付型”合约的保险公司、收集影响车辆零部件的磨损数据以提高其质量的汽车制造商。根据 GDPR 第 26 条，两个或两个以上的控制者可以共同决定处理的目的和方式，因此他们被视为共同控制者。在此情况下，他们应清晰地确定各自的义务，特别是在数据主体权利的行使和 GDPR 第 13 条和第 14 条规定的信息提供方面的义务。

数据处理者：指为或以数据控制者的名义处理个人数据的人。数据处理者按照数据控制者的指示收集和处理个人数据，不以自己的名义使用这些数据。例如，在很多情形下，设备制造商和汽车零部件供应商可能会以汽车制造商的名义处理数据（但这并不意味着他们不会因其他目的而成为数据控制者）。除了要求数据处理者实施恰当的技术和组织措施来确保一个与风险匹配的安全水平，诸如 GDPR 第 28 条还规定了数据处理者的义务。

接收方：指接收向其披露的个人数据的自然人或法人、公共机构、部门或其他主体，不论其是否为第三方。例如，一个服务提供商的商业伙伴从该服务提供商处接收车辆产生的个人数据，该商业伙伴便是个人数据的一个接收方。无论其作为新的数据控制者抑或是作为数据处理者，他们都应当遵守 GDPR 施加的全部义务。

然而，公共机构遵守欧盟法或成员国法律的要求，在一项特定调查的框架下

接收个人数据时，其不被认为是接收方；公共机构对这些数据的处理应根据处理的目的遵守相应的数据保护规则。例如，执法机构根据欧盟法或成员国法律在调查中要求提供个人数据时，他们是被授权的第三方。

1.5 隐私和数据保护风险

第 29 条工作组已经表达过对物联网（IoT）系统的担忧，这些对联网车辆同样适用。[23]已经强调的 IoT 相关的数据安全和控制有关的问题在联网车辆的语境下甚至更为敏感，因为它还会引发车辆环境下道路安全方面的担忧，并且可以影响驾驶员的身体健康，而车辆环境在传统上被视作是一个独立的、免受外部干扰的环境。

此外，联网车辆在位置数据的处理上引发了强烈的数据保护和隐私担忧，因为它不断增加的侵入性质可对目前保持匿名的可能性造成压力。EDPB 想要特别强调并唤起利益相关者的意识：位置技术的使用需要实施特定的保护，以防止对个体的监视和数据的滥用。

1.5.1 缺乏控制和信息不对称

汽车驾驶员和乘客可能并未被充分告知联网车辆的数据处理情况。这些信息可能仅仅提供给汽车的所有人，而汽车所有人可能不是驾驶员，并且可能并未被及时告知这些信息。因此，便存在这样一种风险：受影响的个体行使控制权以利用其数据保护和隐私权利的功能或选项不足。这一点是重要的，因为在其生命周期中，车辆可能会有不止一个占有人，或许因为被出售，或许因为被租用而不是被购买。除此之外，车辆越来越多地被公司或个人共享或出租，被收集数据的人可能无法拒绝某些数据处理。[24]

还有，车内通信可以在个人没有意识到的情况下，被自动或默认触发。在缺乏方法来有效控制汽车和其连接的设备之间的交互时，用户控制数据流动必定会

[23] WP29 – Opinion 8/2014 on the Recent Developments on the Internet of Things; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
[24] Privacy International – Connected Cars: What Happened to Our Data on Rental Cars; https://privacyinternational.org/sites/default/files/2017-12/cars_briefing.pdf

十分困难。控制其后续使用、防止潜在的功能蠕变甚至会更加困难。

1.5.2 用户同意的质量

EDPB 强调，当数据处理是基于同意时，必须符合有效同意的全部要素，也就是说同意应当是自由给出、具体和知情的，并且构成数据主体的愿望的明确表示，正如 EDPB 在关于同意的指南里所解释的那样。[25]数据控制者需要仔细注意从不同参与者处，例如汽车所有人或汽车使用人处，获取有效同意的形式。该种同意必须分开提供，为特定目的并且不能与新车买卖或出租合同绑定。撤回同意必须与给出同意一样简单。

《电子隐私指令》所要求的同意同样适用上述条件，例如特定情形下《电子隐私指令》第 5 条第 3 款要求的存储信息或访问已经存储在车内的信息时。实际上，正如上文所述，在此语境下的同意应当按照 GDPR 来解释。

在很多情形下，用户可能注意不到在其车内进行的数据处理活动。这种信息缺乏对证明 GDPR 下的有效同意构成实质性的阻碍，因为同意必须符合知情条件。在这种情况下，不能以同意作为 GDPR 下相应的数据处理的法律依据。

用于获取个人同意的经典机制在联网车辆环境下难以适用，导致缺乏信息基础的“低质量”同意，或事实上不能根据个人表达的偏好提供调整的同意。实践中，在二手车、出租、借用车辆的情况下，驾驶员和乘客与车辆的所有人没有关系，此时驾驶员和乘客的同意也难以获得。

1.5.3 个人数据的进一步处理

基于《电子隐私指令》第 5 条第 3 款的同意或第 5 条第 3 款的豁免来收集数据时，只有在控制者为其他目的寻求额外同意，或数据控制者可以证明其是基于欧盟或成员国的法律维护 GDPR 第 23 条提及的目标时，这些数据才可以被进一步处理。EDPB 认为，在这些情形下，无法根据 GDPR 第 6 条第 4 款基于兼容性

[25] Article 29 Working Party – WP259 rev.01 - Guidelines on consent under Regulation 2016/679; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 - endorsed by the EDPB

测试而采取进一步处理，因为会破坏《电子隐私指令》的数据保护标准。

EDPB 回顾道，初始同意永远不能使进一步处理合法化，获取同意前必须告知并且同意必须特定方有效。

例如，在为维修目的而使用车辆的过程中所收集的遥测数据，用户未同意创建驾驶员资料以向其提供基于驾驶行为的保险单时，该数据不能向机动车保险公司披露。

此外，当满足执法指令中的特定条件时，联网车辆收集的数据可能会被执法机构处理，用以探测超速或其他违法行为。在这种情况下，根据 GDPR 第 10 条的条件和其他适用的国内立法，该类数据会被视为与刑事定罪和犯罪有关。制造商可能会向执法机构提供该类数据，如果该类处理的特定条件得到满足。EDPB 指出，仅为满足执法机构要求而进行的个人数据处理不构成 GDPR 第 5 条第 1 款 b 项意义上的特定、明确和合法的目的。当执法机构经过法律授权，他们可以成为 GDPR 第 4 条第 10 款意义上的第三方，在此情况下，为遵守各成员国相关法律框架，制造商有权向他们提供其所支配的数据。

1.5.4 过度数据收集

随着装配到联网车辆上的传感器的数量不断增加，与为达成目的所需的数据收集相比，存在很高的过度数据收集风险。

新功能，特别是基于机器学习算法的功能的开发可能需要长期收集大量的数据。

1.5.5 个人数据安全

联网车辆提供的多元的功能、服务和界面（例如网页，USB，RFID，Wi-Fi）增加了攻击面，因此增加了潜在漏洞的数量，这些漏洞可能会危及个人数据。与多数物联网设备不同，联网车辆是关键系统，安全漏洞可能会危及用户和周围人的生命。因此，解决黑客试图利用联网车辆漏洞的风险更为重要。

除此之外，存储在车辆上和/或外部地点（例如云计算基础设施）的个人数据，它们可能没有得到充分的、使其免于未授权访问的安全保护。例如，在维修

期间，一辆汽车必须交由技术人员，该技术人员会要求访问车辆的部分技术数据。当技术人员需要访问技术数据时，存在他试图访问车内存储的全部数据的可能性。

2. 一般性建议

为了减轻上述已识别的对数据主体造成的风险，车辆和设备制造商、服务提供商或其他与联网车辆有关的可能作为数据控制者或数据处理者的利益相关者应当遵循下述一般性建议。

2.1 数据类型

正如在序言中所提及的，大多数与联网车辆相关的数据会被视为个人数据，只要其可能关联到一个或多个可识别的个人。它包括关于车辆运动的技术数据（例如速度、行使距离）以及车辆状况数据（例如发动机冷却液温度、发动机转速、轮胎气压）。鉴于其敏感性和/或对数据主体权益的潜在影响，应当对联网车辆产生的某些数据予以特别关注。目前，EDPB 认定了三种汽车和设备制造商、服务提供商和其他数据控制者应当特别关注的个人数据类型，分别是：位置数据、生物识别数据（和 GDPR 第 9 条规定的特殊数据类型）以及可揭露犯罪行为或交通违法的数据。

2.1.1 地理位置数据

收集个人数据时，汽车和设备制造商、服务提供商和其他数据控制者应当牢记，地理位置数据尤其能够揭示数据主体的生活习惯。已完成的旅程十分有特点，它使得人们可以推断出工作地点和居住地，以及驾驶员的兴趣（休闲）中心，还可能揭示敏感信息，例如通过礼拜地点判断宗教，或通过逗留过的地点推断性取向。相应的，汽车和设备制造商、服务提供商和其他数据控制者应当特别警惕，不要收集位置数据，除非对于处理目的而言绝对必要。例如，当处理行为在于探测车辆运动时，陀螺仪足以满足该项功能，而不必收集位置数据。

总之，收集地理位置数据需要遵守以下原则：

– 对相对于处理目的而收集的地理位置数据的访问频率、细节程度进行充

分的配置。例如，天气应用不应当每一秒都访问车辆的地理位置，即使其获得了数据主体的同意；

- 提供关于处理目的的准确的信息（例如是否存储地理位置历史？如存储，存储目的是什么？）；
- 当处理是基于同意时，获取有效（自由、具体和知情的）同意，该同意的获取与出售或使用的通用条件不同，例如可通过车载计算机获取；
- 仅当用户启动一个要求获取车辆位置的功能时，方可激活地理位置，不可在车辆启动时以默认和持续的方式激活；
- 告知用户地理位置已被激活，特别是以使用图标的方式（例如在屏幕上移动的箭头）；
- 随时禁用地理位置的选项；
- 确定一个有限的存储期限；

2.1.2 生物识别数据

在联网车辆的语境下，生物识别数据可能被用来进入车辆，验证驾驶员/车主身份，和/或访问驾驶员的资料设置和偏好设置。在考虑使用生物识别数据时，保证数据主体对其涉及的数据具有完全的控制，一方面，提供非生物识别的替代方案（例如使用一个物理钥匙或密码）而没有额外的约束（也就是说，生物识别的使用不应当是强制性的），另一方面，仅以本地方式、以加密的形式存储和比对生物识别模板，使生物识别数据不被外部的读取/比对终端处理。

在生物识别数据的场景下，确保生物识别认证解决方案的足够可靠是重要的，特别是通过遵守以下原则来确保：

- 对使用的生物识别解决方案所进行的调整（例如，假阳性和假阴性的比率）适应于必备的访问控制的安全水平；
- 所使用的生物识别解决方案是基于能抵御攻击（例如用平面印刷品进行指纹识别）的传感器的；

– 有限的验证尝试次数；

– 生物识别模板/模型存储在车辆内，以加密的方式，使用最先进的密码算法和钥匙管理；

– 对构成生物识别模板和用于用户验证的原始数据进行实时处理，即使在本地也不对其进行存储。

2.1.3 揭露犯罪行为或其他违法行为的数据

联网车辆的个人数据可能可以揭露某项罪行或其他违法行为（“罪行相关数据”），因此受到特殊限制。例如，与精确的地理位置数据结合的一辆车的瞬时速度，或表明汽车越过一条白线的数据可能被视作罪行相关数据。因此，根据 GDPR 第 10 条，对该类数据的处理仅能在官方机构的控制下或当处理经过欧盟法或成员国国内法授权时，并且为数据主体的权利和自由提供了适当保护时，方可进行。EDPB 认为瞬时速度本身不是罪行相关数据，因为速度限制在各地不同，其自身不能单独揭露一项罪行。然而，这类数据可能会因其收集目的而成为罪行相关数据（例如，为调查和起诉刑事犯罪之目的），在此情况下适用 GDPR 第 10 条规定的保护措施。

为了处理关于潜在犯罪的数据，EDPB 建议采取本地数据处理，此时数据主体对所涉数据具有完全的控制权（参见上文第 2.1 节关于本地处理的讨论）。实际上，除了某些例外情形（参见下文第 3.2 节关于事故防范学的案例研究），禁止对揭露犯罪行为和其他违法行为的数据进行外部处理。因此，根据数据的敏感程度，如第 2.7 节中描述的强有力的安全措施必须得到落实，从而保护数据免于非法访问、修改和删除。

2.2 目的

个人数据可能会因各种各样的和联网车辆有关的目的而被处理，这些目的包括驾驶员安全、保险、高效的交通、娱乐或信息服务。根据 GDPR，数据控制者必须确保他们的目的是“特定、明确和合法的”，不会以与这些目的不一致的方式进一步处理这些数据，并且如 GDPR 第 5 条所要求的那样，其处理具备有效

的法律依据。一些数据控制者在联网车辆环境下运营所寻求的目的的具体示例参见本指南第三部分的讨论，该部分还为每种处理类型提供了具体的建议。

2.3 相关性和数据最小化

为了遵守数据最小化的原则，汽车和设备制造商、服务提供商和其他数据控制者应当特别注意他们所需要的联网车辆的数据类型，因为他们只能收集与处理相关和必要的个人数据。例如，位置数据尤其具有侵入性，可以揭示数据主体的很多生活习惯。因此，行业参与者应当特别警惕，不去收集位置数据，除非这样做对于实现处理目的来说绝对必要（参见上文第 2.2 节关于地理位置数据的讨论）。

2.4 设计和默认的数据保护

考虑到联网车辆产生的个人数据的数量和多样性，EDPB 注意到，数据控制者应当通过承担 GDPR 第 25 条规定的设计的和默认的数据保护义务，确保其在联网车辆环境下部署的技术配置尊重个人隐私。技术设计应以最小化个人数据的收集，提供保护隐私的默认设置和确保数据主体得到充分告知并且可以选择以简易的方式修改与其个人数据相关的配置为目的。关于制造商和服务提供商如何遵守设计和默认数据保护的具体指南对行业来说是有益的。

某些通用实践，如下文所述，也可以帮助减轻联网车辆相关的、对自然人权利和自由的风险。

2.4.1 个人数据的本地处理

总体上，汽车和设备制造商、服务提供商和其他数据控制者应当，如可行，使用不涉及个人数据或不涉及传输个人数据到车外的流程（例如，数据在内部进行处理）。这种场景的优点在于保证用户对其个人数据的唯一和全部控制权，正因如此，它体现了“通过设计”实现的较少的隐私风险，特别是通过禁止利益相关者在数据主体不知情的情况下进行数据处理。这也使得敏感数据诸如生物识别数据或关于犯罪行为或其他违法行为的数据，以及详细的位置数据的处理得以进行，否则这些数据的处理需要遵守更为严格的规则（见下文）。同样，这也会带

来更少的网络安全风险、较小的延迟，使其尤其适合自动驾驶辅助功能。一些此类解决方案的示例可能包括：

- 在车内处理数据的环保驾驶应用，在车载屏幕上实时显示环保驾驶建议；
- 涉及在用户的完全控制下（例如通过蓝牙或 Wi-Fi）传输个人数据到一台设备（例如智能手机）上的应用，并且车辆的数据不会传输给应用提供商或汽车制造商；这包括，比如，连接智能手机以使用汽车的显示、多媒体系统、麦克风（或其他传感器）打电话等，只要收集的数据保持在数据主体的控制之下，并且仅用来提供数据主体要求的服务；
- 车载安全增强应用，例如在驾驶员超车却没有打信号或驶出白线时提供方向盘声音信号或振动，或就车辆状况提出预警（例如，就影响刹车片的磨损提出预警）；
- 使用驾驶员的生物识别数据解锁、启动和/或激活某些车辆指令的应用，这些生物识别数据存储在车内（例如面部或声音模型或指纹特征）。

如上所述的这些应用涉及自然人为纯粹个人活动而进行的处理（即不传输个人数据给数据控制者或数据处理者）。因此，根据 GDPR 第 2 条第 2 款，这些应用不在 GDPR 的适用范围。

汽车制造商和服务提供商应当考虑本地数据处理，只要其能减少云处理的潜在风险，第 29 条工作组在其发布的关于云计算的意见中强调了云处理的潜在风险。[26]

然而，虽然 GDPR 不适用于一个自然人在纯粹个人或家庭活动中所进行的个人数据处理，但其适用于控制者或处理者，他们为该类个人或家庭活动处理个人数据提供了手段（汽车制造商、服务提供商等）。因此，当他们作为数据控制者或数据处理者时，他们必须开发安全的车载应用，并且遵守设计和默认隐私的原则。无论何时，根据 GDPR 导言（Recital）第 78 条，“在开发、设计、挑选和

[26] WP29 – Opinion 5/2012 on Cloud Computing; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

使用基于个人数据处理或处理个人数据以完成任务的应用、服务和产品时，应当鼓励产品、服务和应用的制造商在开发和设计该类产品、服务和应用时把数据保护权利纳入考虑，并适当考虑先进技术，确保控制者和处理者能够履行其数据保护义务”。一方面，它会增强以用户为中心的服务的开发，另一方面，会促进和保证未来后续使用的安全，后续使用可能会落入 GDPR 的适用范围。更具体地说，EDPB 推荐开发一个安全的车载应用平台，与安全相关的汽车功能进行物理分离，以便对汽车数据的访问不依赖于不必要的外部云能力。

通常，用户应当能够控制他们的数据在车辆中被收集和处理的方式：

- 关于处理的信息必须以驾驶员所使用的语言提供（包括手册，设置等）；
- EDPB 建议，只有对于车辆运行所必需的数据才能被默认处理。对于任一其他目的和控制者/处理者，数据主体都应可以激活或停用该数据处理，并且可以删除有关数据；
- 数据不能传输给任何第三方（即，用户拥有对数据的唯一访问权）；
- 数据的保存时间不得超过提供服务所需的时间，或欧盟或成员国法律规定的时间；
- 数据主体应能在出售车辆前永久删除所有个人数据；
- 数据主体可以在可行的情况下直接访问这些应用程序生成的数据。

最后，虽然不是每一用例都可诉诸于本地数据处理，但通常可以采取“混合处理”的方式。 例如，在基于驾驶行为的保险中，关于驾驶行为的个人数据（例如，施加在制动踏板上的力度、行驶的里程数等）既可以在车辆内部处理，也可以由车载信息系统服务提供商（telematics service provider）代表保险公司（数据控制者）进行处理，并生成分数，将这些分数按一个确定的周期（例如按月）传输给保险公司。这样一来，保险公司无法访问原始的行为数据，而只能访问作为处理结果的总分。这可以确保数据最小化的原则从设计着手得到满足。这也意味着，当数据由其他方存储时，用户应当具有行使其权利的能力，例如，用户应具有删除存储在汽车维修店或经销商系统中的数据的能力。

2.4.2 匿名化（anonymization）与假名化（pseudonymisation）

如果数据必须离开车辆，则应考虑在传输之前将其匿名化。EDPB 回顾说，数据保护原则不适用于匿名信息，即无法关联到已识别或可识别的自然人的信息，或使数据主体无法被识别的匿名化的个人数据。一个数据集一旦被真正的匿名化，并且个人无法再被识别，则不再适用欧洲的数据保护法。因此，在相关的地方采取匿名化，可能是保持联网车辆优势并减轻相关风险的好策略。

正如第 29 条工作组在 2014 年 4 月通过的关于匿名化技术的意见中所详述的那样，为了达到数据匿名化的目的，可以使用各种方法，有时可以组合使用这些方法。[27]

考虑到在大多数情况下，不需要直接可识别的数据即可达到处理目的，因此，例如假名化等其他技术可以帮助将数据处理产生的风险最小化。假名化包括用非象征性（non-signifying）的假名代替直接识别的个人数据，例如，假名化可以通过使用密钥哈希算法（secret-key hash algorithm）实现。如有安全保障措施作为增强，假名化通过减少滥用的风险，从而增进对个人数据的保护。与匿名化不同，假名化是可逆的，假名化后的数据仍被视为受 GDPR 约束的个人数据。

2.4.3 数据保护影响评估

考虑到通过联网车辆生成的个人数据的规模和敏感性，处理个人数据，尤其是在车辆外部进行处理的情况下，可能会给个人的权利和自由带来高风险。在这种情况下，将会要求行业参与者按照 GDPR 第 35 条和第 36 条的规定，完成数据保护影响评估（DPIA），以识别和减轻风险。即使在不需要进行 DPIA 的情况下，在设计阶段尽早开展评估亦是最佳实践。这将使行业参与者可以在推出新技术之前将分析结果纳入他们的设计选择中。

2.5 信息提供

[27] WP29 - Opinion 05/2014 on Anonymisation Techniques; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

在处理个人数据之前，应告知数据主体关于数据控制者（例如，车辆和设备制造商或服务提供商）的身份、处理目的、数据接收方、数据存储期限以及 GDPR 下数据主体的权利。

此外，车辆和设备制造商、服务提供商或其他数据控制者还应以清晰、简单且易于访问的方式向数据主体提供以下信息：

- 数据保护官（data protection officer）的联系方式；
- 个人数据的处理目的以及处理的法律依据；
- 当数据控制者或第三方的合法利益构成处理的法律依据时，载明这些合法利益；
- 个人数据的接收方或接收方类型，如有；
- 个人数据的存储期限；或者，如果不可行，则提供用于确定该期限的标准；
- 数据主体有权向控制者请求访问、更正或删除关于数据主体的个人数据，或限制、反对其处理，以及数据主体享有数据可携带权；
- 在以同意为基础进行数据处理的情况下，数据主体有权随时撤回同意，撤回之前基于同意所做的处理的合法性不受影响；
- 在适用的情况下，控制者计划将个人数据传输到第三国或国际组织的事实，以及用于传输的安全保障措施；
- 提供个人数据是否是法定要求、合同要求，或者签订合同所必需的要求，数据主体是否有义务提供该个人数据以及未能提供该数据的可能后果；
- 是否存在自动化决策，包括可能对数据主体产生法律影响或类似的严重影响的用户画像、相关逻辑的有意义的信息以及此类处理对数据主体的重要性和预期后果。这与向个人提供基于驾驶行为的保险而言尤为相关；
- 向监管机构投诉的权利；

– 有关进一步处理的信息；

– 在存在共同数据控制者的情况下，每个数据控制者清晰、完整的责任信息；

在一些情况下，个人数据并非是直接从有关个人处收集而来。例如，车辆和设备制造商可能依靠经销商来收集有关车辆所有者的信息，以便提供紧急路边援助服务。如果未直接收集数据，则车辆和设备制造商、服务提供商或其他数据控制者除了需要提供上述信息外，还应指明有关个人数据的类型、个人数据的来源以及，如果适用，这些数据是否来自可公开访问的来源。上述信息必须由控制者在获取该数据后的合理时间内提供，并且根据 GDPR 第 14 条第 3 款的规定，**不得晚于以下日期中最早的日期**：（1）鉴于处理个人数据的具体情况，获得数据后一个月；（2）首次与数据主体进行通信时；或（3）如果要将这些数据传输给第三方，在传输数据之前。

当有新的数据控制者对数据主体负责时，例如在数据主体跨过边境的情况下，则可能还需要向数据主体提供新的信息。与联网车辆进行交互的路边援助服务可以由不同的数据控制者提供，取决于需要援助时所在的国家或地区。当数据主体跨越边界且与联网车辆进行交互的服务由新的数据控制者提供时，新的数据控制者应向数据主体提供必需的信息。

向数据主体提供信息可以分层提供 [28]，即分成两个层次的信息：一方面是，对数据主体最为重要的第一层信息；另一方面，可能在稍后阶段会有用的信息。重要的第一层的信息包括：数据控制者的身份、数据处理的目的、对数据主体权利的描述以及其他关于对数据主体影响最大的处理或让他们意想不到的处理的信息。EDPB 建议，在联网车辆的情况下，应使数据主体在第一层信息中了解到所有的接收方。如第 29 条工作组在关于透明性的指南中所述，控制者必须提供对数据主体最有意义的接收方有关的信息。实际上，这通常是接收方的名字，以便数据主体准确地知道是谁拥有其个人数据。如果控制者无法提供接收方的名字，

[28] Article 29 Working Party - WP260 rev.01 - Guidelines on transparency under Regulation 2016/679. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 - endorsed by the EDPB

则信息应尽可能明确，指明接收者的类型（即参考其执行的活动）、行业、领域和子领域以及接收者的位置。

这些信息可以在车辆销售合同、服务提供合同和/或任何书面介质中，以简洁易懂的条款，并通过使用不同的文件（例如，车辆维护记录簿或手册）或车载计算机的方式告知数据主体。

根据 GDPR 第 13 和 14 条的要求，除了必要的信息外，还可以使用标准化的图标，通过潜在地减少向数据主体提供大量书面信息的方式来提高透明度。这些图标在车辆中应是清晰可见的，以便提供与计划的处理相关的、易于理解且清晰易读的概览。EDPB 强调了标准化这些图标的重要性，从而使得无论车辆的品牌或型号如何，用户都可以找到相同的标志。例如，当某些类型的数据，例如地理位置正在被收集时，可以在车内显示一个清晰的信号（例如车内的一个灯），以告知乘客数据收集的存在。

2.6 数据主体的权利

车辆和设备制造商、服务提供商和其他数据控制者应通过提供特定工具，促进数据主体在整个处理期内对其数据的控制，提供有效的方法以行使他们的权利，特别是访问权、更正权、删除权、限制处理的权利以及视处理的法律依据而定的数据可携带权和反对权。

为了便于对设置进行修改，应该在车辆内部安装用户配置文件管理系统，以便存储已知驾驶员的偏好并帮助他们随时轻松地更改其隐私设置。车辆中的配置文件管理系统应对每项数据处理的每个数据设置进行集中，尤其在数据主体提出要求时，方便其访问、删除和迁移个人数据。除非特别法律法规另有规定或者数据对于车辆的关键功能至关重要，否则应使驾驶员能够随时临时或永久停止收集某些类型的数据。

联网汽车的出售以及随之而来的所有权变更也应当触发删除所有的个人数据，这些数据对于之前的具体目的而言不再必要。

2.7 安全性与保密性

车辆和设备制造商、服务提供商和其他数据控制者应采取措施，确保其处理的数据的安全性和保密性，并采取一切有用的预防措施，防止其被未经授权的人员控制。行业参与者应尤其考虑采取以下措施：

- 使用最先进的算法对通信通道进行加密；
- 为每辆车（而不是每个型号）建立独有的加密密钥管理系统；
- 当远程存储时，使用最先进的算法对数据进行加密；
- 定期更新加密密钥；
- 保护加密密钥不被泄露；
- 验证数据接收设备；
- 确保数据完整性（例如，通过哈希（hashing））；
- 访问个人数据应使用可靠的用户身份验证技术（密码、电子证书等）；

特别是对于汽车制造商，EDPB 建议实施以下安全措施：

- 将车辆的重要功能与那些始终依靠通信能力的功能（例如“信息娱乐”）区分开来；
- 实施技术措施，使汽车制造商在车辆的整个使用寿命内能够迅速修复安全漏洞；
- 对于车辆的重要功能，应尽可能优先使用专门用于交通运输的安全频率；
- 设置一个防止车辆系统受到攻击的预警系统，并可在降级模式运行；
- 存储访问车辆信息系统的日志记录，例如，最长可以追溯到六个月前，以便理解任何潜在攻击的来源，并定期检查日志信息以发现可能的异常情况。

这些一般性建议应搭配特定要求来完成，顾及每项数据处理的特征和目的。

2.8 向第三方传输个人数据

原则上，只有数据控制者和数据主体才能访问由联网车辆生成的数据。但是，数据控制者可能会将个人数据传输给商业伙伴（接收方），前提是这种传输是基于 GDPR 第 6 条所述的法律依据之一。

车辆制造商、服务提供商或其他数据控制者可以将个人数据传输给一个数据处理者，该数据处理者被选择参与向数据主体提供服务，但前提是该数据处理者不得将这些数据用于其自身目的。数据控制者和数据处理者应起草合同或其他法律文件，明确各方的义务并约定 GDPR 第 28 条的规定的内容。

考虑到车辆使用行为数据（vehicle-usage data）的敏感性（例如，完成的旅程、驾驶风格），EDPB 建议，在将数据主体的数据传输给作为数据控制者的商业伙伴之前，应按部就班地获得数据主体的同意（例如，通过在未打勾的方框上打勾，或者在技术上可行的情况下，通过人们可在车辆中使用的物理或逻辑设备）。反过来，商业伙伴对其接收的数据负责，并受 GDPR 所有规定的约束。

2.9 向欧盟/欧洲经济区之外传输个人数据

当个人数据被传输到欧洲经济区之外时，应采取特殊的安全保障措施以确保保护措施随数据一起转移。

因此，数据控制者只能在符合 GDPR 第五章的条件的范围内，将个人数据传输给接收方。

2.10 车载 Wi-Fi 技术的使用

蜂窝技术的进步使得在旅途中轻松使用互联网成为可能。尽管可以通过智能手机热点或专用设备（OBD-II 适配器、无线调制解调器或路由器等）在车内实现 Wi-Fi 连接，但当今大多数制造商都提供了包含内置蜂窝数据连接的模型，并且还能够创建 Wi-Fi 网络。根据实际情况，必须考虑各个方面：

- Wi-Fi 连接作为道路从业人员（例如出租车司机）为其顾客提供的一项服务。在这种情况下，该从业人员或其公司可能会被视为互联网服务提供商（ISP），因此在处理其客户的个人数据方面要遵守特定的义务和限

制。

– Wi-Fi 连接仅供驾驶员使用（不包括其乘客）。在这种情况下，对个人数据的处理被视为纯粹的个人或家庭活动。

通常，Wi-Fi 的网络连接接口的激增给个人隐私带来了更大的风险。实际上，通过他们的车辆，用户成为持续的广播者，并因此可以被识别和跟踪。为了防止被跟踪，车辆和设备制造商必须采用易于操作的退出选项，确保车载 Wi-Fi 网络的服务集标识符（SSID）不被收集。

3. 案例研究

本章介绍了在联网车辆中进行处理的五个具体示例，这些示例与行业的利益相关者可能遇到的场景相对应。这些示例涵盖了数据处理（该数据处理需要计算无法在车辆中本地调动的能力），和/或向第三方发送个人数据以进行进一步的分析或远程提供其他功能。对于每种类型的处理，本文都明确了其处理目的、所收集数据的类型、此类数据的存储期限、数据主体的权利、要实施的安全措施以及信息的接收方。如下文对其中某些方面未进行描述，则适用前文的一般性建议。

所选择的示例并非详尽无遗，旨在显示可能在联网车辆的环境中存在的处理类型、法律依据、参与者等的多样性。

3.1 由第三方提供服务

数据主体可以与服务提供商签订合同，以获得与他们的车辆有关的增值服务。例如，数据主体可能会签订一份“按里程付费”（Pay As You Drive）保险合同，该种合同为良好的驾驶行为提供降低的保险费，而且保险公司需要监控驾驶习惯。数据主体还可以与一家在车辆发生故障时提供路边援助的公司签订合同，因此需要将车辆的位置传输给该公司或一家服务提供商，以便接收有关车辆功能的消息或警报（例如，有关制动器磨损状态的警报，或关于技术检查日期的提醒）。

3.1.1 按里程付费（PAYD）保险

按里程付费是一种基于驾驶行为的保险，它可以跟踪驾驶员的里程和/或驾

驶习惯，通过向其提供降低的保费来区分和奖励“安全”的驾驶员。保险公司会要求驾驶员安装一个内置的车载信息服务，该服务可追踪投保人的行驶里程和驾驶行为（制动方式、快速加速等）。车载信息服务设备收集的信息将用于给驾驶员打分，以便分析他们可能给保险公司带来的风险。

EDPB 概括，按里程付费类型的保险应该始终是非强制的，投保人必须有权选择非基于驾驶行为的保险。

3.1.1.1 法律依据

当数据是通过公共电子通信服务（例如，通过车载信息服务设备中包含的 SIM 卡）收集而来时，根据《电子隐私指令》第 5 条第 3 款，需要征得同意才能访问已存储在车辆中的信息。实际上，这些规定所提供的任何豁免在此情况下都无法适用：该处理并非仅为通过电子通信网络进行通信传输的目的，也不是与消费者或用户明确要求的信息社会服务有关。同意可以在签订合同时取得。

根据 GDPR 第 6 条第 1 款 b 项，在特定情况下，保险公司可以对在存储或访问终端用户的终端设备之后进行个人数据处理，前提是它可以证明处理是在与数据主体签订有效合同的情况下进行的，并且处理对于履行与数据主体签订的该特定合同而言是必要的。仅限于处理对于履行与数据主体所签订合同而言是客观必要的这种情况，EDPB 认为，依据 GDPR 第 6 条第 1 款 b 项的处理不会降低《电子隐私指令》第 5 条第 3 款中对于这种特定情况所提供的额外保护的效果。数据主体与保险公司之间签订了合同，构成了其处理的法律基础。

3.1.1.2 收集的数据

有两种类型的个人数据需要考虑：

- **商业和交易数据：**数据主体的识别信息、与交易有关的数据、与支付方式有关的数据等；
- **使用行为数据：**车辆产生的个人数据、驾驶习惯、位置等。

EDPB 建议，鉴于存在车载 T-BOX 收集的数据被滥用，从而导致对驾驶员活动进行精确画像的风险，因此必须尽可能以下列方式之一处理有关驾驶行为的

原始数据：

- 把数据留在车内的车载 T-BOX 中或用户的智能手机中，从而使保险公司只能访问结果数据（例如，关于驾驶习惯的分数），而不能访问详细的原始数据（请参阅第 2.1 节）；
- 或由车载信息服务提供商代表控制者（保险公司）生成分数，把分数按确定的周期传输给保险公司。在这种情况下，原始数据和直接与驾驶员身份有关的数据必须分开。这意味着车载信息服务提供商虽然接收实时数据，但不知道投保人的姓名、车牌等。另一方面，保险公司知道投保人的姓名，但仅接收分数和总公里数，而不接收用于产生此类得分的原始数据。

此外，必须注意的是，如果仅有里程数是履行合同所必需的，那么就不应收集位置数据。

3.1.1.3 保存期限

在为履行合同而进行数据处理的情况下（即提供服务），重要的是先区分这两种数据，然后再确定各自的保存期限：

- **商业和交易数据：**可以在合同的整个有效期内将这些数据存储在主动数据库中。合同结束时，可以将它们进行物理归档（在单独的介质上：CD-ROM 等），或逻辑存储（通过授权管理），以备可能的诉讼之需。此后，在法定时效期限结束时，应对数据进行删除或匿名化；
- **使用行为数据：**使用行为数据可以分为原始数据和聚合数据（aggregated data）。如上所述，如可行，数据控制者或处理者不应处理原始数据。如有必要，原始数据的保存期限以被要求制作聚合数据和检查该聚合过程的有效性的期间为限。聚合数据的保存期限以提供服务所需和欧盟或成员国法律的另行规定为限。

3.1.1.4 信息提供和数据主体的和权利

在处理个人数据之前，根据 GDPR 第 13 条的规定，应当以透明且易于理解

的方式告知数据主体。特别是，必须告知数据主体其个人数据的存储期限，或者，如不可行，则告知用于确定该期限的标准。在最后这种情况下，EDPB 建议采取一种教育方法（pedagogic approach），以强调原始数据与以此为基础得出的分数之间的差异，并强调保险公司只会在适当的情况下收集分数的结果。

如果数据不是在车辆内部处理，而是由车载信息服务提供商代表控制者（保险公司）处理的，则提供信息时可以有用地提及，在这种情况下，提供商无法访问与驾驶员身份直接相关的数据（例如姓名、车牌等）。此外，考虑到告知数据主体处理其个人数据的后果的重要性，以及处理个人数据的行为不应使数据主体感到意外，EDPB 建议，应当告知数据主体用户画像的存在，以及这种画像的后果，即使它不涉及 GDPR 第 22 条所提到的任何自动决策。

至于数据主体的权利，应明确告知他们行使其访问、更正、限制和删除权的可行方法。由于在此环境下收集的原始数据是由数据主体提供的（通过特定形式或通过其行动），并且数据处理是建立在 GDPR 第 6 条第 1 款 b 项（合同的履行）基础之上，因此，数据主体有权行使其数据可携带权。正如在数据可携带权指南中所强调的那样，EDPB 强烈建议："数据控制者应清楚地说明数据主体通过行使访问权和数据可携带权可接收到的数据类型之间的差异"。

可在签订合同时提供信息。

3.1.1.5 接收方

EDPB 建议，应尽可能在车载 T-Box 中直接处理车辆的使用行为数据，以便保险公司仅能访问结果数据（例如一个分数），而不是详细的原始数据。

如果一个车载信息服务提供商代表数据控制者（保险公司）收集数据以生成分数，则其无需知道投保的驾驶员的身份（例如姓名，车牌等）。

3.1.1.6 安全

适用第 2.7 节的一般性建议。

3.1.2 停车位的租赁和预订

如停车位的所有人欲出租自己的车位，他会在一个网页应用上挂出停车位并为其定价。一旦挂出该停车位，当有驾驶员想要预订时，该应用便会通知停车位的所有人。驾驶员可以选择一个目的地并可基于多种标准来查询可用的车位。在得到车位所有人的批准后，交易即被确认，服务提供商处理付款事宜，然后使用导航驾驶汽车到该位置。

3.1.2.1 法律依据

通过公开可用的电子通信收集数据时， 适用《电子隐私指令》第 5 条第 3 款的规定。

因为本示例属于一种信息社会服务，当服务是由订阅者明确要求的，《电子隐私指令》的第 5 条第 3 款并不要求取得同意才可访问已经存储在车辆中的信息。

对于处理个人数据和并且仅针对为履行与数据主体签订的合同所必要的数据而言， GDPR 第 6 条第 1 款 b 项是其法律依据。

3.1.2.2 收集的数据

处理的数据包含驾驶员的联系信息（姓名，电子邮件，电话号码，车辆类型（如汽车、卡车、摩托车）、车牌号、停车时长、支付信息（例如信用卡信息）以及导航数据。

3.1.2.3 保存期限

数据的保存期限以履行泊车合同所需和欧盟或成员国法律的另行规定为限。此后，应对数据进行匿名化处理或删除。

3.1.2.4 信息提供和数据主体的权利

在处理个人数据之前，必须按照 GDPR 第 13 条规定，以透明、易懂的方式告知数据主体。

必须明确告知数据主体其行使访问、纠正、限制和删除权的可行方法。鉴于在这种情况下是数据是从数据主体处（通过特定形式或通过数据主体的行动）收

集而来，且数据处理是建立在 GDPR 第 6 条第 1 款 b 项（合同的履行）基础之上，数据主体有权行使其数据可携带权。正如在数据可携带权指南中所强调的，EDPB 强烈建议“数据控制者清楚说明数据主体通过数据访问权和数据可携带权可接收到的数据类型之间的差异”。

3.1.2.5 接收方

原则上，只有数据控制者和数据处理者可以访问数据。

3.1.2.6 安全

适用第 2.7 节的一般性建议。

3.2 紧急呼叫（eCall）

在欧盟境内发生严重事故时，车辆会自动触发 eCall 拨打欧盟紧急求助电话 112（具体内容见第 1.3 节），从而将救护车及时地派到事故发生地。这依据的是 2015 年 4 月 29 日欧盟第 2015/758 号关于部署基于 112 服务的车载自动紧急呼叫系统的型式批准要求的条例，该条例对第 2017/46/EC 号指令进行了修订。

事实上，安装在车内的 eCall 生成器（generator）可以通过公共移动无线通信网络进行数据传输，发起紧急呼叫。仅在发生事故时，该紧急呼叫可由车辆传感器自动触发，也可以由车内人员手动触发。除了激活音频渠道外，事故自动触发的第二个事件包括生成最小数据集（MSD）并将其发送到公共安全应答点（PSAP）。

3.2.1 法律依据

在适用《电子隐私指令》时，必须考虑到以下两个条款：

- 第 9 条：关于仅适用于电子通信服务的交通数据以外的位置数据。
- 第 5 条第 3 款：访问车内安装的生成器中存储的信息。

尽管原则上这些条款要求数据主体的同意，但 2015 年 4 月 29 日的欧盟 2015/758 号条例仍构成数据控制者应遵守的法律义务（当数据主体无法做出真实

自由的选择，并且其无法拒绝对其的数据的处理）。因此，根据欧盟 2015/758 号条例在处理位置数据和最小数据集（MSD）[29]时不一定要获取驾驶员的同意。

处理这些数据的法律依据要符合 GDPR 第 6 条第 1 款 c 项中所规定的义务（即欧盟 2015/758 号条例）。

3.2.2 收集的数据

欧盟 2015/758 号条例规定，基于 112 的车内紧急呼叫系统发送的信息应仅包括欧盟标准 EN 15722:2015“智能运输系统—智能安全—eCall 最小数据集（MSD）”中的最小信息，包括：

- 表明 eCall 是自动或人为触发的数据；
- 车辆类型；
- 车辆识别号（VIN）；
- 车辆动力类型；
- 当前 eCall 事件中的初始数据消息生成的时间戳；
- 在消息生成前最后时刻确定的最新已知车辆经纬度；
- 在消息生成前最后时刻确定的最新已知车辆行驶实时方向（仅包含汽车最后三个位置）。

3.2.3 保存期限

欧盟 2015 年 4 月 29 日的第 2015/758 号条例规定，数据保存期限不得超过处理紧急情况所需的时间。当数据不再为上述的目的所必须时，应当将其完全删除。此外，应自动且不断删除在 eCall 系统内部存储器中的数据。只有车辆最后三个位置的数据可以被储存，仅限于用于明确车辆的当前位置和事故发生时车辆

[29] It has to be noted that Article 8-1-f of the last version of the working document of the proposal for an “ePrivacy” regulation does provide a specific exemption for eCall as consent is not needed when “it is necessary to locate terminal equipment when an end-user makes an emergency communication either to the single European emergency number ‘112’ or a national emergency number, in accordance with Article 13(3).”

的行驶方向所绝对必要的程度。

3.2.4 信息提供和数据主体权利

2015 年 4 月 29 日的欧盟 2015/758 号条例的第 6 条规定，制造商应提供关于使用 eCall 系统所进行的数据处理的清晰、完整的信息。在使用 eCall 系统之前，应在用户手册中针对基于 112 的车载 eCall 系统和由第三方服务支持的 eCall 系统分别提供上述信息，包括：

- 数据处理的法律依据的证明；
- 基于 112 的车载 eCall 系统是默认激活的；
- 基于 112 的车载 eCall 系统所开展的数据处理的安排；
- eCall 处理的特定目的，应仅限于第 5 条第 2 款第 1 段规定的紧急情况；
- 收集和处理的数据的类型以及该数据的接收方；
- 基于 112 的车载 eCall 系统中的数据的保存期限；
- 不会持续跟踪车辆；
- 关于行使数据主体权力和负责处理访问请求的联络服务的安排；
- 提供第三方服务 eCall 和/或其他增值服务相关的任何关于个人数据的可追踪性、对该个人数据的跟踪、处理的其他必要信息，这些信息的提供应取得所有人的明示同意且遵守 GDPR 的规定。应特别考虑以下事实：通过基于 112 的车载 eCall 系统与车载第三方服务 eCall 系统或其他增值服务进行的数据处理之间可能存在差异。

此外，服务提供商还应根据 GDPR 第 13 条的要求，以透明、易懂的方式向数据主体提供信息。特别是应告知数据主体处理其个人数据的目的，以及个人数据的处理是基于数据控制者所承担的法律义务这一事实。

此外，考虑到数据处理的性质，有关个人数据接收方和接收方类型的信息必须是清楚明确的，并且应告知数据主体，在触发 eCall 之前，除了基于 112 的车

载 eCall 系统之外，任何实体都无法获得其数据。

至于数据主体的权利，必须指出，鉴于数据处理是建立在法律义务之上的，拒绝权和可携带权在此处不适用。

3.2.5 接收方

在触发 eCall 之前，除了基于 112 的车载 eCall 系统之外，任何实体都无法获得该数据。

当 eCall 系统被触发时（由车内人员手动或在车载传感器检测到严重碰撞时自动触发），eCall 系统将与相关的 PSAP 建立语音连接，并将 MSD 发送给 PSAP 运营商。

此外，仅在发生与 eCall 相关的事件以及满足第 585/2014/EU 号决议的条件下，且数据仅用于实现该决议的目标的情况下，才可以将通过基于 112 的车载 eCall 系统传输并由 PSAP 处理的数据传输给第 585/2014/EU 号决议规定的紧急服务和服务合作伙伴。未经数据主体事先明确同意，不得将 PSAP 通过基于 112 的车载 eCall 系统处理的数据传输给任何其他第三方。

3.2.6 安全

欧盟第 2015/758 号条例规定，将加强隐私保护的要求纳入 eCall 系统技术当中，以便为用户提供适当水平的隐私保护和防止监视、滥用的保障。此外，制造商应确保基于 112 的 eCall 系统以及其他提供 eCall 的系统（由第三方服务或增值服务处理的）的设计使得个人数据无法在这些系统间进行交换。

关于 PSAP，成员国应确保保护个人数据免遭滥用（包括非法访问、更改或丢失），建立适当程度的有关个人数据的存储、保存期限、处理和保护的规则，并遵守上述规则。

3.3 事故防范学研究

数据主体可自愿参与事故防范学研究，该研究是为了更好地了解道路事故的起因或出于更一般的科学目的需求。

3.3.1 法律依据

当数据是通过公共电子通信服务收集时，**根据《电子隐私指令》第 5 条第 3 款的规定，如访问已存储在车辆中的数据，**数据控制者必须收集数据主体的同意。事实上，上述条款中的任何例外情况在这里都不适用：此类处理并非仅为通过电子通信网络来达成传输通信目的，也与用户、订阅者明确要求的信息社会服务无关。

考虑到事故防范学研究所需的个人数据的多样性和数量，根据 GDPR 第 6 条的规定，个人数据处理应获取数据主体的事先同意。该事先同意必须以特定形式做出，用以表明数据主体自愿参与研究并同意以此目的处理其个人数据。同意应是相关数据主体对其自由、具体和知情的意愿的表达（例如，在空白方框上打勾，或配置车载计算机以激活车辆的一个功能）。该同意必须针对其特定目的而单独提供，不得与购买或租赁新车的合同捆绑，并且同意必须如同提供一样易于撤回。撤回同意将导致停止处理，随后应将数据从主动数据库中删除或进行匿名化处理。

《电子隐私指令》第 5 条第 3 款要求的同意与作为数据处理法律依据的同意可以被同时收集（例如以在框中打叉的方式，明确表示数据主体所同意的内容）。

3.3.2 收集的数据

数据控制者仅应收集为处理所绝对必要的个人数据。

有两种数据类型需要考虑：

- 与参与者和车辆相关的数据；
- 车辆的技术数据（例如瞬时速度）。

事故防范学相关的科学研究是收集瞬时速度数据的正当性基础，包括由一个从严格意义上来说并不管理公共服务的法人来收集数据的情况。

如上所述，EDPB 认为在事故学研究中收集的瞬时速度数据从目的上来说并非犯罪相关数据（即并非出于调查或起诉犯罪的目的而收集），因此，即使由一个严格意义上非管理公共服务的法人来收集该数据也是具备正当性的。

3.3.3 保存期限

区分这两种类型的数据是十分重要的。首先，与参与者或者车辆相关的数据可在研究期间内保存。其次，车辆的技术数据的保存期限不能超出自研究结束之日起 5 年的时间。上述期限过后，应当将数据删除或作匿名化处理。

3.3.4 信息提供和数据主体权利

在处理个人信息之前，应当根据 GDPR 第 13 条的要求以透明、易懂的方式告知数据主体。特别是在收集瞬时速度的情况下，应明确告知数据主体该数据收集。由于数据处理是基于同意的，因此必须明确告知数据主体其有权随时撤回同意，在撤回之前基于同意已经做出的数据处理的合法性不受影响。此外，由于在这种情况下收集的数据是由数据主体提供的（通过特定形式或通过其活动），并且处理基于 GDPR 第 6 条第 1 款 a 项（同意）而进行的，因此数据主体有权行使其数据可携带权。正如在数据可携带权指南中所强调的那样，EDPB 强烈建议，“数据控制者清楚说明数据主体通过数据访问权和数据可携带权可接收到的数据类型之间的差异。”因此，数据控制者必须提供一种简便的方式让数据主体可以随时自由地撤回其同意，数据控制者也应开发能够响应数据可携带权请求的工具。

信息可在签署同意参加事故防范学研究表格时提供。

3.3.5 接收方

原则上，只有数据控制者和数据处理者可以访问数据。

3.3.6 安全

如上所述，采取的安全措施应与数据敏感程度匹配。例如，如果在事故防范学研究中收集了瞬时速度（或与刑事定罪和犯罪相关的任何其他数据），EDPB 强烈建议采取强有力的安全措施，例如：

- 实施假名化措施（例如，对诸如数据主体的姓/名和序列号的数据进行密钥哈希（secret-key hashing data））；

- 将瞬时速度有关的数据和地理位置数据分别存储在单独的数据库中（例如，使用具有不同密钥和批准机制的先进的加密机制）；
- 和/或在参考事件或序列符合条件（例如，道路类型，白天/夜晚）且直接识别的数据存储在只能由少数人访问的单独数据库中时，立即删除地理位置数据。

3.4 应对汽车盗窃

在发生汽车盗窃时，数据主体可能希望尝试使用地理位置来查找其车辆。在这种情况下，位置数据的使用仅限于调查必需和主管法律部门对案件的评估。

3.4.1 法律依据

通过公共电子通信服务收集数据时，适用《电子隐私指令》第 5 条第 3 款。

因为本示例是一种信息社会服务，当服务是由订阅者明确要求的，《电子隐私指令》的第 5 条第 3 款不要求取得同意才可获取已存储在车辆中的信息。

此时，个人数据处理的法律依据是车辆所有人的同意，或者，如果适用，为合同的履行（仅限为履行与车辆所有人签署的合同所必需的数据）。

同意应是相关数据主体的自由、具体和知情的意愿的表达（例如，在空白方框上打勾，或配置车载计算机以激活车辆的一个功能）。应明确告知数据主体，给出同意的自由包括可随时选择撤回同意。撤回同意将导致数据处理终止。在这之后应将数据从主动数据库中删除、匿名或归档。

3.4.2 收集的数据

位置数据仅能在宣布遭到盗窃时传输，不得在其余时间连续收集位置数据。

3.4.3 保存期限

位置数据只能在主管法律部门进行案件评估期间进行保存，或保存至消除怀疑的程序结束为止。该程序并不随着确认车辆被盗而结束。

3.4.4 向数据主体提供信息

在处理个人数据之前，应当根据 GDPR 第 13 条的规定以透明且易懂的方式告知数据主体。具体地说，EDPB 建议数据控制者应强调其不会对车辆进行持续跟踪，且位置数据只能在宣布被盗时才能被收集和传输。此外，控制者必须向数据主体提供有关以下事实的信息：只有经批准的远程监控平台人员和法律批准的机构才能访问该数据。

关于数据主体的权利，由于该数据处理是以同意为基础，因此必须明确告知数据主体其有权随时撤回同意。在撤回之前基于同意已经做出的数据处理的合法性不受影响。此外，由于在这种情况下收集的数据是由数据主体提供的（通过特定形式或通过其活动），并且处理是基于 GDPR 第 6 条第 1 款 a 项（同意）或第 6 条第 1 款 b 项（合同的履行）而进行的，因此，数据主体有权行使其数据可携带权。正如在数据可携带权指南中强调的，EDPB 强烈建议，“数据控制者清楚说明数据主体通过访问权和可携带权可接收到的数据类型之间的差异。”

因此，数据控制者必须提供一种简便的方法（仅在同意为其法律依据的情况下），使数据主体可以随时自由地撤回其同意，并开发能够响应数据可携带权请求的工具。

上述信息可在签订合同时提供。

3.4.5 接收方

在宣布被盗时，位置数据可传输给（1）经批准的远程监控平台人员，和（2）法律批准的机构。

3.4.6 安全

适用第 2.7 节中的一般性建议。

3.5 存储在租赁车辆仪表盘上的个人信息

租用车辆时，数据主体可能希望使用其车载娱乐功能，例如导航到给定的目的地，拨打电话或播放音乐。上述功能的实现要依靠多种技术手段，并且存在之前的车内人员的数据对后续用户亦可见的风险。

3.5.1 已收集的数据

各种各样的数据可在租赁车辆的仪表盘内进行处理。这些数据可在以下情况下被处理：

- 当数据主体的智能手机与租赁车辆的仪表盘配对后，例如使用蓝牙或USB 连接（电话标识符，语音和数据通信等）；
- 当驾驶员或乘客使用租赁车辆的仪表盘时（GPS 导航历史，网页浏览以及越来越多的应用程序）。

因此，生成的数据可以揭示个人信息（网页浏览数据、联系人、日程表，音乐、广播和其他流音频或视频内容的选择等），并可以有助于生成精准的数据主体的画像。[30]

鉴于汽车租赁公司对处理具有控制权，其应被视作该信息（存在于租赁的车辆仪表盘上的信息）的数据控制者，故租车公司有责任确保数据保密和遵守数据保护合要求。

3.5.2 向数据主体提供信息

为了使用户能够有效地控制其数据，租赁公司必须向用户提供清楚明确的信息，包括可能在本地进行处理的数据、数据处理的目的以及随时停止数据收集并删除有关数据的选项。例如，假如车辆仪表盘上配备了一个“删除按钮”，租赁公司必须提示用户关注该功能。

3.5.3 保存期限

EDPB 建议制造商提供一个简单的功能（例如删除按钮），使数据主体可以快速轻松地从汽车的仪表盘上移除其个人数据。

租赁公司应当制定清晰的内部程序，用于在再次出租车辆之前清除存储在车

[30] Privacy international, Connected Cars: What Happens To Our Data On Rental Cars?; https://privacyinternational.org/sites/default/files/2017-12/cars_briefing.pdf

辆仪表盘上的个人数据。

3.5.4 安全

租赁公司应确保租赁车辆仪表盘上的权限设置是符合设计的和默认隐私的原则的（具有防止第三方处理汽车仪表盘生成的数据的设置，仅在第三方征得用户同意时才允许其为特定目的访问该数据）。