洞见

罗兰贝格

02.2022
上海 / 中国

软件定义汽车下的个人隐私保护

——场景驱动模式落地

Roland Berger

前言

在技术、政策、用户需求等共同作用下，软件定义汽车的进程已经进入深水区。更先进的电子电气架构、更大更智能的计算芯片、更灵活的软件以及云服务等成为未来智能网联汽车发展的重要驱动力。作为物联网 (IoT) 终端和智慧交通的核心组成部分，智能网联汽车将产生大量数据。仅一辆自动驾驶汽车每小时产生的数据量就达 80-100GB，每天产生的数据量为 TB 级别。与此同时，随着传感器和车载芯片数量的增多，数据埋点也急剧增加。大量的数据埋点和海量的数据处理和传输大幅增加了网络安全和数据泄露的风险，尤其是个人隐私数据。此外，政策在权责边界框定、标准制定和场景细化方面加速落地。

近日，罗兰贝格通过梳理近 60 条国际与国内隐私保护相关法律法规与行业标准，分析跨行业近 20 个隐私保护案例，并与政策制定者、主机厂、零部件供应商、独立网络安全服务商进行广泛、深入的探讨，发布《软件定义汽车下的个人隐私保护白皮书》。报告以案例为切入点，分析智能网联汽车个人隐私保护的三大发展趋势，旨在就此课题为业界带来全新视角。

目录

1 / 产业链玩家接连碰壁

2017 年 1 月，某图商发布报告，披露了某品牌车主偏好的活动场所类型，该用户画像的公开引发部分车主的声讨。事件在该图商修改报告措辞后逐渐沉寂。

2021 年 4 月，某车主在车辆行驶过程中刹车失灵，而厂家为自证刹车运行良好，未经允许向媒体公布了该车主的刹车数据，被车主指控侵犯其个人隐私，并引发社会对此事件的激烈讨论。最终，该车主并未向有关部门投诉，事件逐渐被淡化。

5 月，多个品牌的二手车在交易后，原车主依然能访问 APP 并获取相关信息，即车辆同时绑定了新、老车主的手机号，导致新车主的信息泄漏。6 月，有主机厂回应称问题已在解决，将尽快上线相关功能。

7 月，某移动出行巨头 IPO 上市，因涉及潜在的个人信息过度收集与处理而引发数据出境调查。国家网信办指其违规收集个人信息，已进驻实施安全审查；期间，该公司系列 APP 下架，新用户不得注册。→ 01

01 / 近年各行业隐私保护案例[1)]

	车主刹车信息被未经允许公开	出行平台违规收集个人信息	某品牌车主活动场所偏好被披露	车辆交易后原车主仍可远程访问
事件基本信息	• 某新势力品牌车主认为车辆刹车失灵并诉诸媒体，厂商未经用户允许公开刹车数据以自证清白	• 某移动出行巨头境外上市后，被核实存在严重违规收集个人信息行为，产品强制下架	• 某图商在公开发布的消费者画像报告中，提及某品牌车主特定的活动场所偏好，引发部分车主强烈不满	• 多家品牌二手车新车主称车辆过户后，原车主账号并未强制解绑，依然可远程访问车辆
事件分析	• 车主与厂商对刹车数据是否属于个人信息存在不同认知 • 彼时尚无相应法规出台，监管部门难以给出明确意见	• 消费者担忧该公司对个人信息收集程度、使用方式等存在泄露风险 • 有明确法规规定，对违规收集个人信息的企业须进行审查与处罚	• 消费者对数据如何收集表示困惑，图商也并未披露数据来源 • 法规明确规定不可精准定位至个人，但品牌群体是否同样适用难界定	• 买卖双方对解绑缺少了解，相关车企在车机/APP设计时也缺乏对车辆交割后信息安全的关注 • 法规尚未出台，监管难以评判
时间发展脉络	2021.4 车主维权 车企公布车主行车数据 车主控诉侵犯隐私，要求撤销数据并道歉 车企公布刹车记录以自证清白，随后市值受到波动 车主未向有关部门投诉，不了了之	2021.6 该移动出行巨头申请境外IPO上市 2021.7 网信办进行网络安全审查，期间停止新用户注册 该公司紧急更新隐私协议 七部门进驻开展安全审查 个人信息保护法第三次审议	2017.1 图商发布报告，提及某品牌车主偏好活动场所 部分车主发文指责该图商以偏概全 图商修改报告措辞，但未回应舆论	2021.5 某品牌二手车新车主称车辆系统升级需要原车主授权 2021.6 又一品牌车主称，车辆与APP绑定后无法取消 车企回应正在解决，将上线新功能进行完善

1) 提及案例的所有信息均为公开披露，并隐去了相关名称

资料来源：案头研究；罗兰贝格

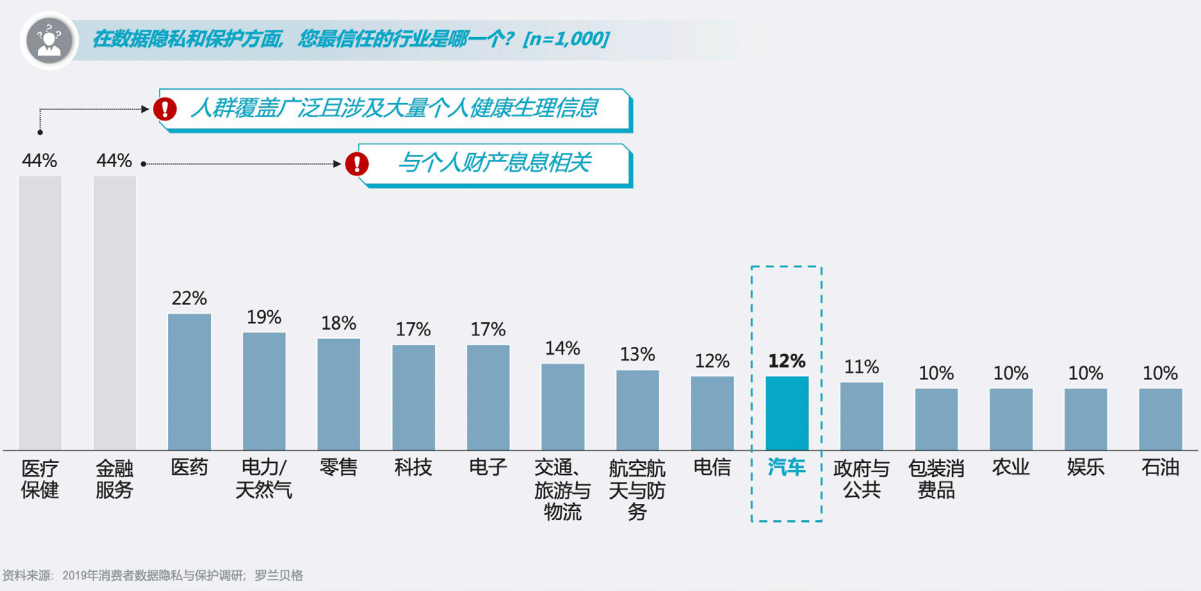
2 / 智能网联汽车个人隐私保护迎来拐点

上述四个案例涉及智能网联汽车产业链条上的不同玩家，且有着一个共同之处，即受制于执法依据不充分、社会舆论不强等掣肘，隐私风险问题最终多“不了了之”或“尚未定论”。同时，由于智能网联汽车的技术处于萌芽与迭代期，尚未形成行业统一的产业化实践，相关法律法规仍在陆续出台且具体实施细则及解读仍待发布，类似信息安全事件发生后存在“只点名，不处罚”等现象。

与传统的消费电子、泛网络通信等相比，智能网联汽车额外产生大量与智能座舱、自动驾驶、V2X 等相关的全新数据类型，如车内外环境及位置轨迹、生物识别数据等。而全球各类玩家在开展业务时，由于相关法规在近两年的快速出台，在合法合规性上也面临着各式各样的风险，接连碰壁。

但不容忽视的是，随着车内联网服务的增加，未来消费者对于个人隐私保护的顾虑将愈发凸显。消费者的意识与关注是触发隐私纠纷的关键因素之一。目前，相比于医疗、金融等其他行业，消费者对汽车行业的隐私保护信任度较低。智能网联汽车所涉及的隐私风险场景与互联网、通讯行业愈发相似，而针对捆绑服务迫使用户同意、信息过度采集与处理等风险尤为如此。→ 02

02 / 不同行业的数据隐私和保护度



通过上述四个案例管中窥豹，可以肯定的是，汽车领域隐私泄露事件的频发与消费者隐私保护意识的觉醒将驱动立法落地，行业即将迎来拐点。

3 / 智能网联汽车个人隐私保护三大发展趋势

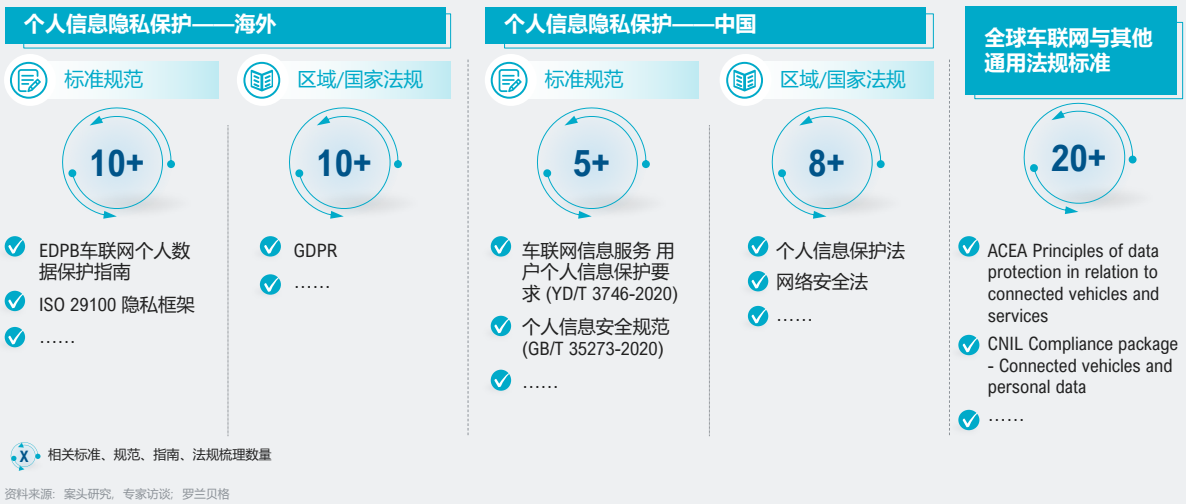
长期以来，罗兰贝格与领先主机厂、供应商、独立网络安全与信息安全服务商，以及相关政策制定机构进行深入探讨。我们认为，未来智能网联汽车个人隐私保护将呈现三大趋势。第一，立法进程加速细化，并呈现全球多个法规体系共存的格局。第二，主机厂应对合规风险，分化不同发展风格。第三，隐私保护将场景化发展，驱动具体的隐私保护模式和功能落地。→ 03

03 / 三大发展趋势

趋势一：立法进程加速细化，全球多个法规体系共存

罗兰贝格通过梳理全球隐私保护相关的法律法规（全球超过 20 项，中国超过 10 项），以及全球车联网与通讯相关的法律法规（全球和中国均超过 10 项），观察到中国的立法进程正处于从“框定边界”向“法规细化”演进的时期。未来，中国个人信息隐私保护立法将对标欧美领先国家实践，逐步形成包含标准、规范、指南、法规等多层级的完备立法体系。值得期待的是，监管部门将陆续出台个人信息保护的立法细则，针对智能网联汽车发展过程中已经暴露或潜在的风险问题，及时补充适用性准则，同时对标参照欧美个人信息隐私保护领域领先立法，不断填充我国隐私保护立法领域的空白，形成立法体系雏形。例如，以网安法为总纲领逐步细化落地的车联网用户个人信息保护要求 (YD/T 3746-2020)、个人信息保护法和汽车数据安全管理若干规定等。→ 04

04 / 全球相关法律法规与标准梳理（不完全列举）



与此同时，各个国家在网络安全与隐私保护上的法律法规进展并不一样，尤其在车联网领域的各项定义（如个人信息和个人敏感信息等）未形成一致口径，存在多个法规体系共存。例如，ISO 29100，GDPR 和《个人信息保护法》都是从最高层面对个人信息保护提出指导原则；而 EDPB 和 YD/T 3746 则分别是基于 GDPR 和个保法所衍生的在车联网领域较细化的指南和规范。不同法规体系主要有以下三点不同：

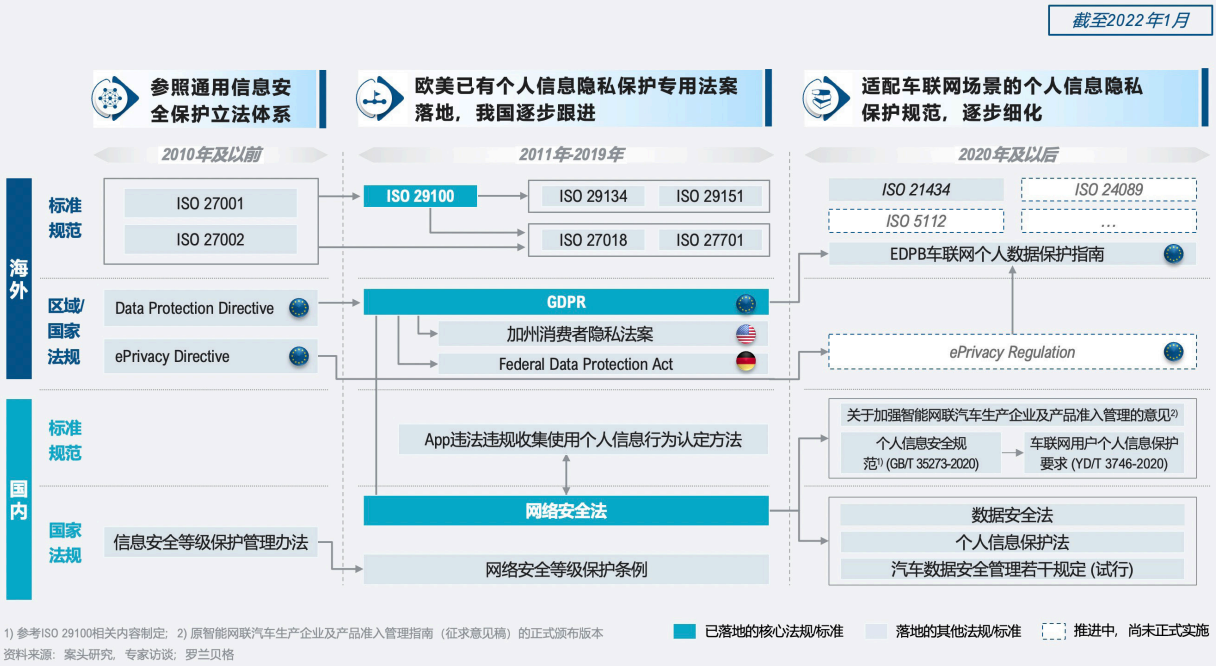
1. 不同法规体系对个人信息的定义方式不同。例如，GDPR 和个人信息保护法对个人数据的定义是“与可识别自然人相关的信息”，而 ISO 29100 的定义为“能够单独或者与其他信息结合能够识别公民个人身份的各种信息”。这两种定义方式在逻辑上存在差异，前者称为“识别 + 相关”，后者则称为“识别”。

2. 对个人敏感信息的定义与分层略有不同。在 ISO 29100，GDPR 与《个人信息保护法》中均划分出了“个人敏感信息”的类目，但由于文化、国情等差异，不同法规在个人敏感信息的定义逻辑上存在不同。例如，《个人信息保护法》定义的敏感信息不包括 GDPR 所强调的“政治观念”；同时，《个人信息保护法》又将诸如“婚史”、“金融账户”和“未成年人信息”等纳入“敏感”范畴。

3. 在车联网领域里，对个人信息和个人敏感信息的定义颗粒度和细化程度在各法规中均不相同。国内主要参考《车联网个人信息保护要求》，其中《车联网个人信息保护要求（YD/T 3746）》对个人信息敏感性作三层分级，而海外法规采用的是个人信息 + 敏感信息二层分级方式。

我们认为，不同国情、政治、文化与治理框架使得不同法规体系共存。这意味着企业全球化战略中必须考量不同区域市场的法规要求，提前进行法规研究、合规性认证以及与监管部门必要的前期沟通，以避免全球化进程受到合规问题的阻碍。→ 05

05 / 国内外个人信息隐私保护立法演进



1) 参考ISO 29100相关内容制定；2) 原智能网联汽车生产企业及产品准入管理指南（征求意见稿）的正式颁布版本

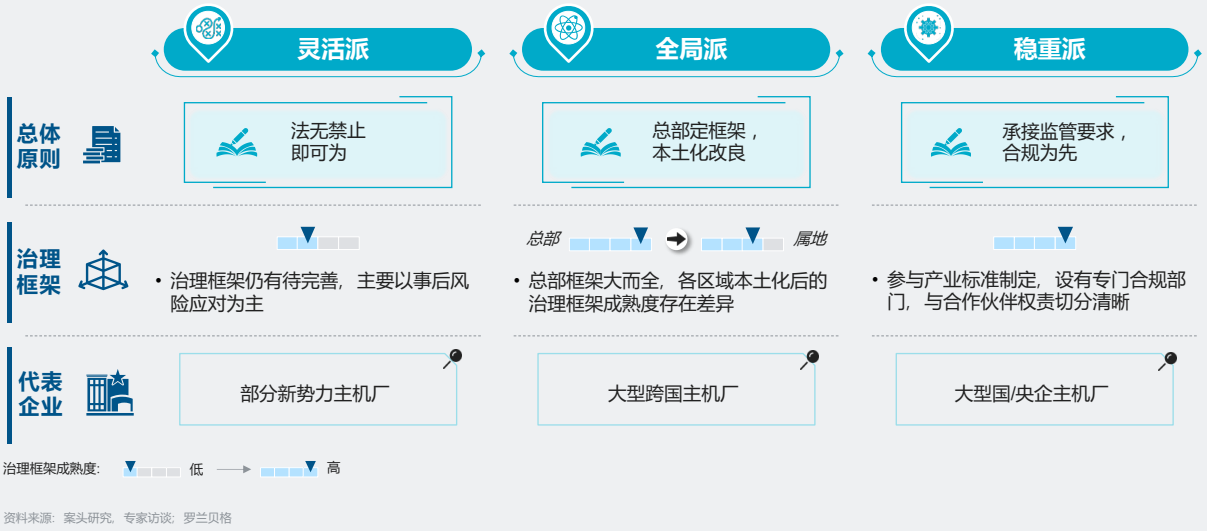
资料来源：案头研究，专家访谈；罗兰贝格

趋势二：主机厂应对合规要求，分化不同发展风格

网络安全与隐私保护已成为主机厂及其他车联网产业从业者在全球化进程中面临的重要课题。面对各项法律、标准、规定等，国内外主机厂挑战重重。网络信息安全与隐私保护已然跻身为与碳中和、芯片和半导体同一层级的导致全球化进程增速放缓的重大因素，成为国内外厂商共同面临的难题。

为应对挑战，不同类型的玩家也在不断尝试，摸索各自的“生存模式”与风格。以部分新势力主机厂为代表的“灵活派”，偏倾向于“法无禁止即可为”，在法规尚处模糊地带时采取相对大胆的做法，但同时也准备好风险应对机制；以大型跨国厂商为代表 “全局派”，则在总部层面设计一个大而全的网络安全与隐私保护框架，并在各国布设团队以完成相关本土化工作；而以国/央企主机厂为代表的“稳重派”，作为中国车联网产业标准制定的主要参与方，响应上层管理部门号召，在网络安全与信息保护方面与各合作伙伴有着较明确的权责切分，规范化程度高。→ 06

06 / 主机厂合规应对路线



资料来源：案头研究，专家访谈；罗兰贝格

趋势三：场景化发展驱动隐私保护模式和功能落地

在政策、玩家、消费者的合力作用下，车联网产业的隐私保护将以车辆生命周期与风险类别为双主线，并以场景化模式进行逐层推进与小步快跑式迭代。在场景的不断丰富、完善与积累下，将在未来迎来转折点，标志着产业成熟期的步入。隐私保护行业的发展离不开对“风险”的识别和评估，而风险的本质即个人数据在采集、使用、保存、传输、共享、销毁等活动中的泄露或滥用。同时，这些风险在用户购买、使用车辆的全生命周期内不同触点的体现方式和强弱不同。因此，若要更好地保护用户隐私，必须基于车辆生命周期中的各类触点及隐私风险类型，识别具体的隐私风险场景，进而基于场景找到隐私保护的具体模式和功能。此外，在风险场景中还需同步考虑个人信息的敏感性等级。

行业领先的主机厂，尤其是新造车势力和智能网联供应商，已经开始尝试开发针对具体场景的隐私保护功能和模式。以“车辆物权转移场景下的个人数据删除”场景为例，在二手车交易等场景下，或发生车主个人信息清除不彻底或仍可通过云端访问原车主个人信息，导致原车主个人信息

暴露至下一任车主，如账号、密码、地址等个人身份信息、服务或业务订购、个人行踪轨迹、交易记录、好友列表等用户服务信息，导致原车主信息泄露的风险。

该功能具体的实现方式为，在一键解绑车辆后，车内存储的个人身份信息与用户服务信息（包括亲友账号）即时删除，车端恢复出厂设置；此外，该功能提供车主个人信息云端删除的选项，车主可自行选择删除。

该功能值得探讨之处在于，车端和云端均存有个人数据和车辆数据，因此两端的数据删除存在多种选项。同时，对于个人信息的边界，用户与主机厂的定义存在一定差异。而其背后的考量因素包括主机厂和供应商对法律法规的解读（尤其针对当前模糊地带）、对用户运营的重视、对技术迭代的要求等。例如，某本土车联网供应商针对某自主品牌车型，采取“个人信息车端与云端一并删除，仅保留车辆信息”的方式。其数据库构建时将个人信息与车辆信息分开区隔，车主仅能控制个人信息，包括个人身份信息、软件使用偏好、车机使用记录等。而部分豪华品牌主机厂则采取“车端个人信息删除，云端数据视情况而定”的策略，即车机内保存的账户个人信息可以删除，而云端保存的个人信息则不会主动删除，除非个人要求；同时，云端数据定期根据不同数据类型进行清理，而为了训练自动驾驶，其感知融合等算法优化相关信息则不会删除。→ 07

07 / 二手车交易场景下的隐私风险与应对

可以肯定的是，政策法规的成熟与细化将进一步针对类似以上重点场景形成更明确的规定。例如，《汽车数据安全管理若干规定（试行）》中明确“个人要求删除的，汽车数据处理者应当在十个工作日内删除”，《数据安全法》提出“建立数据分类分级保护制度”。因此，数据控制者必须尽快针对数据采集的目的进行数据区隔，明确可删与保留数据的范围。

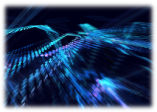
4 / 罗兰贝格为产业玩家提出三大建议

随着智能网联汽车的发展，服务与功能日益增多，个人信息采集的途径与场景也将随之增加。同时，法律法规仍在进一步完善和细化，且全球各个区域的法规体系各不相同。罗兰贝格建议，企业首先应找准自身在数据治理和不同隐私保护场景中的角色，即扮演数据拥有者还是数据处理者；其次，应以法规标准为基线，平衡合规、用户诉求、技术与成本四大要素，开发相应的隐私保护功能与模式；最后，企业应优化隐私治理框架，从治理目标开始，贯穿各业务条线，完善治理维度和详细举措，形成企业自身的标准。→ 08

08 / 罗兰贝格为产业玩家提出的三大建议

明确自身在隐私保护链路中的角色定位

- 例如，作为数据控制者，个人信息采集应具备恰当目的，并确定个人信息采集最小范围，避免因过度采集与处理带来的合规风险



开发均衡型的隐私保护功能与模式

- 以法规标准为基线，合理平衡合规、用户诉求、技术与成本四大要素，开发相应的隐私保护功能与模式，是未来业务需要的新思路

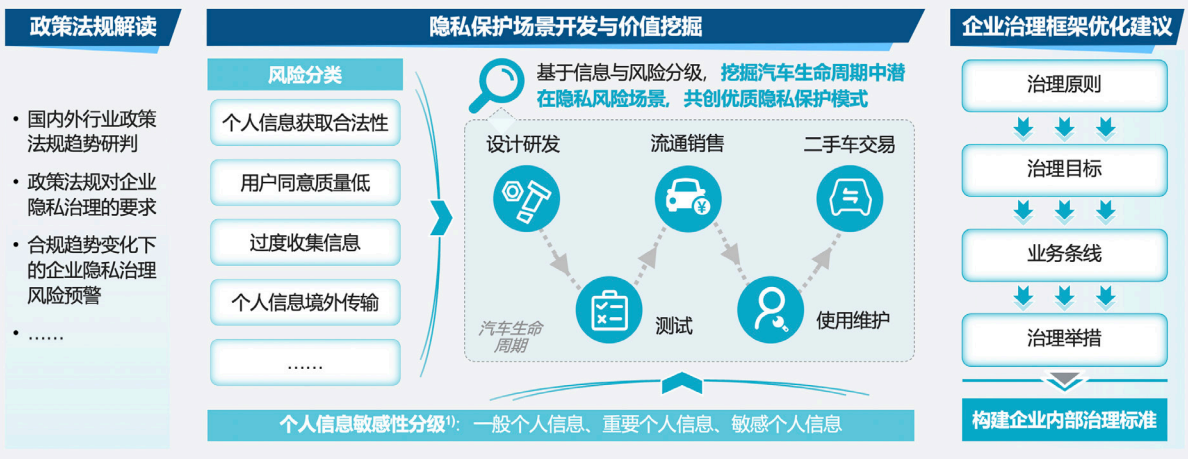
构建自上而下的隐私治理标准

- 优化隐私治理框架，基于整体目标，贯穿各业务条线，完善治理举措，形成治理标准，并以相同标准规范合作方，共同提升隐私保护水平

资料来源：罗兰贝格

罗兰贝格在智能网联汽车用户隐私保护方面具有丰富经验，尤其是基于政策法规解读的隐私保护场景开发与价值挖掘，以及企业隐私治理框架优化等方面，旨在助力行业玩家在隐私保护、数据治理和网络安全领域中实现共赢。→ 09

09 / 罗兰贝格专业能力与服务



1) 参考《车联网个人信息保护要求》定义

作者

郑赟
罗兰贝格全球高级合伙人
ron.zheng@rolandberger.com

时帅
罗兰贝格合伙人
shuai.shi@rolandberger.com

罗兰贝格**张泠荃**对本文亦有贡献。

欢迎联系罗兰贝格汽车团队

郑赟
罗兰贝格全球高级合伙人
ron.zheng@rolandberger.com

戴江宁
罗兰贝格全球合伙人
jiangning.dai@rolandberger.com

袁文博
罗兰贝格全球合伙人
wenbo.yuan@rolandberger.com

吴钊
罗兰贝格全球合伙人
neil.wu@rolandberger.com

时帅
罗兰贝格合伙人
shuai.shi@rolandberger.com

徐虎雄
罗兰贝格合伙人
huxiong.xu@rolandberger.com

赵雯婷 博士
罗兰贝格副合伙人
wenting.zhao@rolandberger.com

庄景乾
罗兰贝格副合伙人
jack.zhuang@rolandberger.com

欢迎您提出问题、评论与建议
www.rolandberger.com

关于我们

罗兰贝格管理咨询公司成立于1967年，是全球顶级咨询公司中唯一一家始于德国、源自欧洲的公司。我们拥有来自34个国家的2400名员工，并成功运作于国际各大主要市场。我们的50家分支机构位于全球主要商业中心。罗兰贝格管理咨询公司是一家由近250名合伙人共有的独立咨询机构。

出版方
罗兰贝格亚太总部
地址：
中国上海市南京西路1515号
静安嘉里中心办公楼一座23楼，200040
+86 21 5298-6677
www.rolandberger.com