

# 《汽车数据出境安全指引（2026版）》

## 你问我答

2026年3月25日

## 编制单位

中国信息通信研究院

国家工业信息安全发展研究中心

中汽智能科技（天津）有限公司

车联网安全集智联盟

中国汽车工业协会

欧洲汽车工业协会

中国电池工业协会

工业信息安全产业发展联盟

中国智能网联汽车产业创新联盟

中国通信标准化协会

中国互联网协会

# 《汽车数据出境安全指引（2026版）》

## 你问我答

为引导汽车数据处理者高效便利安全开展汽车数据出境活动，履行数据安全责任义务，提升数据安全保护水平，依据《汽车数据出境安全指引（2026版）》（以下简称《安全指引》），聚焦汽车数据出境场景下高频热点问题，采用问答的形式，制定本文件。

### 一、基础定义类

#### 1.汽车数据处理者的范围是什么？

答：《安全指引》适用于开展汽车数据处理活动中自主决定处理目的和处理方式的组织、个人，包括汽车制造商、零部件和软件供应商、电信运营企业、自动驾驶服务商、平台运营企业、经销商、维修机构、出行服务企业、地图平台企业、动力电池制造企业等。其他类型企业如满足自主决定汽车数据处理目的、处理方式，也应按照《安全指引》要求履行相关义务。

2.汽车数据中的个人信息范围是什么？按照《安全指引》，个人信息达到多少量级需要申报数据出境安全评估？

答：汽车数据中的“个人信息”包括车主、乘客以及车外摄像头采集的视频、图像中涉及的个人信息。《安全指引》第一部分“总则”明确，非关键信息基础设施运营者向境外提供个人信息（不含敏感个人信息）需申报数据出境安全评估的量级为自当年1月1日起累计100万及以上，敏感个人信息量级为自当年1月1日起累计1万及以上。关键信息基础设施运营者向境外提供个人信息的，应当依法依规申报数据出境安全评估。

3.如果企业A只负责数据的收集和使用，数据的存储、处理等均由另一个企业B（与A为不同法人主体）完成，企业A是否被定义为汽车数据处理者？如果申报数据出境，应当由企业A还是企业B进行申报？

答：《安全指引》第一部分“总则”明确，“汽车数据处理者是指开展汽车数据处理活动中自主决定处理目的、处理方式的组织、个人”。企业 A 自主决定数据的收集和使用，企业 B 自主决定数据的存储、处理，因此，A 和 B 均为汽车数据处理者。无论企业 A 或者企业 B，只要存在汽车数据出境情况，均应当依法依规申报数据出境安全评估、订立个人信息出境标准合同或通过个人信息出境认证。

#### 4.汽车数据处理者如何报告安全漏洞数据？

答：汽车数据处理者应按照《网络安全产品漏洞管理规定》，登录工业和信息化部网络安全威胁和漏洞信息共享平台—车联网产品安全漏洞专业库（NVDB-CAVD）平台（<https://cavd.org.cn>），进入主界面后点击“漏洞报送”，按照平台相关说明进行漏洞信息填报。

#### 5.低中等级漏洞是否也需要先向工业和信息化部报备才可以免于申报数据出境安全评估？

答：《安全指引》第二部分“重要数据判定”明确，涉及高危及以上安全漏洞的未公开的车辆及车联网平台安全漏洞信息以及相关系统名称、系统域名、IP 地址、端口、风险 URL 为重要数据。低中等级漏洞，按照《安全指引》，不属于重要数据。

#### 6. NVDB-CAVD 漏洞库下发的安全漏洞也需要先报备么？

答：对于 NVDB-CAVD 漏洞库下发的安全漏洞，汽车数据处理者也需要登录工业和信息化部网络安全威胁和漏洞信息共享平台—车联网产品安全漏洞专业库（NVDB-CAVD）平台（<https://cavd.org.cn>），进入主界面后点击“通用漏洞出境报告”或“待处置漏洞”，按照平台相关说明进行漏洞信息填报。

#### 7.如果向工业和信息化部报备的企业主体和实际开展出境业务的企业主体不是同一个，涉及安全漏洞数据，是否需要重新报备才可以免于申报数据出境安全评估？

答：向工业和信息化部进行安全漏洞报备的企业主体和实际开展出境业务的企业主体不同的情况下，实际开展出境业务的企业仍需完

成漏洞报备后，才可以免予申报数据出境安全评估。

#### 8.汽车数据处理者如何报告安全事件数据？

答：按照《公共互联网网络安全突发事件应急预案》，汽车数据处理者应当对本单位网络和系统的运行状况进行密切监测，一旦发生网络安全突发事件，应当立即向工业和信息化部网络安全应急办公室和相关省（自治区、直辖市）通信管理局报告；按照《工业和信息化领域数据安全事件应急预案（试行）》，汽车数据处理者认为可能发生较大及以上数据安全事件的，应当立即向地方行业监管部门报告。

#### 9.安全事件数据是否可以在国外的安全领域最佳实践中被公开披露？

答：《安全指引》第二部分“重要数据判定”明确，满足“涉及重大及以上网络和数据安全事件的”即识别为重要数据，但考虑到企业因处置事件的时效性需要，“因处置安全事件需要，按照行业网络安全、数据安全事件相关应急预案，已向工业和信息化部及相关行业监管部门报告的汽车产品、车联网平台及相关系统的安全事件数据”免予申报数据出境安全评估。“最佳实践披露”不属于该场景，如需出境，应当依法依规申报数据出境安全评估。

#### 10.汽车数据处理者如何备案 OTA 升级软件包？

答：汽车数据处理者应按照《缺陷汽车产品召回管理条例》《关于进一步加强智能网联汽车产品准入、召回及软件在线升级管理的通知》等文件要求，通过国家汽车产品召回综合管理信息系统（<http://qczh.samr.gov.cn>）提交备案信息，将电子版升级包以光盘形式邮寄至国家市场监督管理总局缺陷产品管理中心，完成汽车远程升级（OTA）技术备案。

## 二、重要数据判定类

#### 11.如何理解《安全指引》中“重要数据判定”的适用场景？是否只是针对出境业务，企业在其他业务环节中应如何把握？

答：《安全指引》第二部分“重要数据判定”明确了汽车领域重

要数据判定规则，适用于汽车数据处理者开展重要数据识别和目录备案。如果已经识别为重要数据，应该按照《中华人民共和国数据安全法》《数据出境安全评估办法》等法律政策相关要求，履行包括数据出境场景在内的数据全生命周期安全保护义务。

**12.如同一类数据在不同场景下均涉及，应该如何选择适配的重要数据判定规则？**

答：分别针对每个场景，按照数据项、数据项说明确定数据类别，再根据相关判定规则进行数据级别判定，符合任意一条判定规则的，即属于重要数据。

**13.已识别出的重要数据是否禁止出境？**

答：按照《中华人民共和国网络安全法》《中华人民共和国数据安全法》有关要求，汽车数据处理者因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。已经通过数据出境安全评估的重要数据可以出境。

**14.如何理解判定规则中“国家重大专项、国家重点研发计划支持的”的表述？**

答：“国家重大专项、国家重点研发计划”指国家或者有关部门委托研究的重点研发任务或国家科技计划项目，如需要了解更详细的信息，可联系相关委托部门咨询。

**15.“国家重大专项、国家重点研发计划支持的”或者“涉及车联网网络与数据安全、驾驶自动化功能相关成果获得省部级及以上奖励的”是否有时间周期？**

答：没有时间周期，相关数据类别符合“国家重大专项、国家重点研发计划支持的”或者“获得省部级及以上奖励的驾驶自动化相关成果”，无论何时获得的支持或奖励，均属于重要数据。

**16.企业参与了某项国家重点研发计划，但该项研发计划已被列为国家秘密，其相关数据是否属于重要数据？**

答：按照《中华人民共和国数据安全法》第五十三条，开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

#### 17.如何识别汽车动力电池相关重要数据？

答：《安全指引》第二部分“重要数据判定”中的研发设计、生产制造场景明确汽车动力电池相关数据项及重要数据判定规则，汽车数据处理者应先按照数据类别、数据项和数据项说明确定数据分类，再根据判定规则确定数据级别，识别是否属于重要数据。

18.经脱敏处理的数据，是否就可以不用再进行数据级别判定了？

答：经脱敏处理的数据，仍需按照《安全指引》第二部分“重要数据判定”的判定规则进行数据级别判定，如符合“涉及或经汇聚、分析后能推算出军事管理区、国防科工单位及县级以上党政机关等重要敏感区域”等相关判定规则中的任意一项，即属于重要数据。

19.如何理解判定规则中“涉及在境内运行的10万台以上车辆收集的”？该数量是否是去重后的累计数量，还是要包含未来预期？是否包含境内短暂运行，然后就出口境外的车辆？是否区分量产或测试车辆？

答：“涉及在境内运行的10万台以上车辆收集的”中的“10万”，指截至到目前、去重后的累计数量，这个数量指的是在境内短暂或长期运行的量产车或测试车，不包含未来预期。

20.关于“涉及采集真实环境中累计2000小时以上原始影像”和“涉及1000万张以上原始图片”，是否包含公开的数据集？

答：无论是否包含公开数据，均应该按照《安全指引》进行数据级别判定，如符合相关判定规则，即属于重要数据。

21.判定规则中“涉及采集真实环境中累计2000小时以上原始影像”“涉及1000万张以上原始图片”，如果车机采集阶段就已进行了脱敏和匿名化的影像和图片（原始图片/视频已是匿名化处理之后

的），是否不包含在判定规则范围内？

答：相关数据中包含的视频或图片无论是否进行了脱敏或匿名化，均应该按照上述判定规则进行数据级别判定，符合“涉及采集真实环境中累计 2000 小时以上原始影像”或“涉及 1000 万张以上原始图片”的，属于重要数据。

22.关于判定规则中“车外真实人脸边界框最小边长为 32 像素以上”和“车外真实汽车号牌边界框最小边长为 16 像素以上”是否涉及数量要求？广告牌、光滑表面倒映中出现的人脸目标是否属于上述判断规则范围？

答：不涉及数量要求，只要符合判定规则像素要求应当识别为重要数据。广告牌上出现的人脸、光滑表面倒映中出现的人脸目标如果是真实人脸，也应按照判定规则进行数据级别判定。

23.生产制造场景与研发设计场景中的“物料清单”如何区分？判定规则是否通用？

答：分属于研发设计和生产制造两个阶段，二者数据项说明不同，判定规则相同。

24.基于开源人工智能技术的驾驶自动化算法数据，是否属于重要数据？

答：《安全指引》第二部分“重要数据判定”明确，“驾驶自动化算法源代码”指的是“基于人工智能技术的未开源的组合驾驶辅助或自动驾驶算法源代码”，对于基于开源人工智能技术开展自主研发、且最终未作开源处理的驾驶自动化算法源代码，应当依据判定规则开展数据级别判定；如符合相关判定规则，即属于重要数据。

25.车企在与高校、科研机构等联合开展研究过程中产生的驾驶自动化算法相关科研论文成果，是否属于重要数据？

答：按照《安全指引》第二部分“重要数据判定”，先判断论文中是否涉及驾驶自动化算法文件、驾驶自动化算法源代码、驾驶自动化算法参数等数据，如果涉及，按照其判定规则进行数据级别判定，

符合相关判定规则的，属于重要数据。

**26.关于驾驶自动化算法训练数据中的“方向盘转向角、档位信息、刹车踏板开度”是否属于重要数据？**

答：《安全指引》第二部分“重要数据判定”明确，“与车外实景影像、雷达数据融合关联后，符合以下任意一项条件的”属于重要数据，如果只是“方向盘转向角、档位信息、刹车踏板开度”，未与车外实景影像、雷达数据融合关联，不属于重要数据。

**27.驾驶自动化算法训练数据及特征数据的判定规则“涉及采集真实环境中累计 2000 小时以上原始影像的，或者基于此影像生成的”是否为去重的 2000 小时？还是数据处理者所持有 2000 小时？是否与车辆数量有关？**

答：上述判定规则中的累计 2000 小时以上，不需要去重，只要达到时长要求，即属于重要数据，与采集数据的车辆数量无关。

**28.驾驶自动化算法训练数据及特征数据中的判定规则“涉及 1000 万张以上原始图片的，或者基于此图片生成的”是否为去重的 1000 万张？还是数据处理者所持有 1000 万张？是否与车辆数量有关？**

答：上述判定规则中的 1000 万张以上，不是去重后的，只要达到图片数量要求，即属于重要数据，与采集数据的车辆数量无关。

**29.“经过特征提取出的道路标志、标线、车辆、行人目标物等”的图像特征数据是否属于重要数据？**

答：《安全指引》第二部分“重要数据判定”明确，“用于组合驾驶辅助或自动驾驶算法的图像特征数据，包括原始图片、影像数据等经过特征提取出的道路标志、标线、车辆、行人目标物等”，符合“国家重大专项、国家重点研发计划支持的”“经汇聚、分析后能够推算出涉密、敏感地理信息数据的”等 9 项判定规则中的任意一项的，即属于重要数据。

**30.安全驾驶、电池管理以外的软件升级包源代码是否属于重要**

数据？

答：《安全指引》第二部分“重要数据判定”明确，“安全驾驶、电池管理功能升级软件包对应的源代码”，符合相关判定规则的，属于重要数据，安全驾驶、电池管理以外的软件升级包源代码不属于重要数据。

**31.汽车数据处理者升级汽车安全驾驶、电池管理功能，如仅涉及 OTA 软件包不涉及源代码，是否属于重要数据？**

答：《安全指引》第二部分“重要数据判定”明确，“安全驾驶、电池管理功能升级软件包对应的源代码”，符合相关判定规则的，属于重要数据，OTA 软件包不涉及源代码，不属于重要数据。

**32.汽车安全驾驶、电池管理功能的软件包对应的源代码出境需求不是软件升级服务场景，是否就不属于重要数据？**

答：《安全指引》第二部分“重要数据判定”明确，“安全驾驶、电池管理功能升级软件包对应的源代码”，符合相关判定规则的，属于重要数据。场景分类不是进行重要数据识别判定的条件。

**33.面向境外运行车辆提供软件升级包，不涉及境内运行车辆，是否属于重要数据？**

答：题目中提及的升级境外运行车辆，不符合“软件升级数据”的三个判定规则中的“涉及升级境内运行车辆的”，不属于重要数据。

**34.不涉及车辆启动行驶、动力丢失、紧急制动、巡航控制、车道保持、充放电控制、电池温度控制功能的安全驾驶、电池管理功能升级软件包对应的源代码是否属于重要数据？**

答：《安全指引》第二部分“重要数据判定”明确，“软件升级数据”的判定规则包括“涉及车辆启动行驶、动力丢失、紧急制动、巡航控制、车道保持、充放电控制、电池温度控制功能的”，如不符合该条判定规则，不属于重要数据。

**35.单独的车辆识别码（VIN）、车联网卡标识码是否属于重要数**

**据？什么情形下属于重要数据？**

答：《安全指引》第二部分“重要数据判定”明确，符合“与其他出境信息结合可识别个人身份”且“自当年1月1日起向境外提供累计100万人以上”，属于重要数据。单独的车辆识别码、车联网卡标识码，未与其他出境信息结合识别到个人身份，因此不属于重要数据。

**36.公钥证书是否属于重要数据？**

答：《安全指引》第二部分“重要数据判定”明确，符合“涉及在境内运行的10万台以上车辆的远程诊断、更新、通信过程中的根证书”属于重要数据。除了根证书以外的其他公钥证书，不属于重要数据。

**37.境内服务器生成的车辆控制指令下发到车辆过程中产生的日志，是否属于重要数据？**

答：《安全指引》第二部分“重要数据判定”明确，符合相关数据项说明和判定规则的控制指令属于重要数据，如果日志中仅包含不可逆的执行状态数据（如布尔值、时间戳、状态码等），不包含指令本身内容、参数或任何可重构原始指令的信息，不属于重要数据。

**38.国内生产但售往海外的车辆，在车辆出厂时预置了用于境外通信的eSIM配置文件（含IMSI），该IMSI由境外运营商分配且仅在车辆出海后激活，此类IMSI是否也应该按照“车联网卡标识码”的判定规则进行重要数据判定？**

答：《安全指引》第一部分“总则”明确，“在境外收集和产生的汽车数据传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的”，可以免于申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息出境认证。该车辆预置的IMSI是境外传至境内的数据，出厂预置中并未引入境内个人信息或重要数据，因此不属于个人信息或重要数据。

**39.雷达数据中的点云数据已经识别为重要数据，基于点云数据**

**提取的结构化数据是否还需要进行重要数据识别？**

答：《安全指引》第二部分“重要数据判定”明确了“结构化数据”与“点云数据”的数据项说明，点云数据虽已经识别为重要数据，结构化数据仍应按照判定规则进行数据级别判定，如符合判定规则，即属于重要数据。

**40.在封闭测试场（如企业园区、专业试验道路）采集的有限数量的车路感知数据，是否属于重要数据？**

答：封闭测试场采集的有限数量的车路感知数据，也应当进行数据类型和数据项的识别，再按照相关判定规则进行数据级别判定，如符合判定规则，即属于重要数据。

**41.基于已有的道路数据（已确认不在军事管理区、国防科工单位、县级以上党政机关等法定敏感区域内），使用 AI 大模型对未来一个月以上的人员流量或车辆流量数据进行预测，并将预测结果传至境外，是否需要申报数据出境安全评估？**

答：汽车数据处理者应按照《安全指引》第二部分“重要数据判定”，对题目中提及的预测结果数据，进行重要数据识别判定，如属于重要数据且有出境需求，应当依法依规申报数据出境安全评估。

**42.通过手机 APP 或云端平台下发远程控制指令后，车辆内部生成的传动、转向、制动等控制信号数据是否为“车辆控制指令”范围？（例如，手机 APP 发送自动泊车指令，车辆接收到指令后，相关车辆控制器接收到的 CAN/LIN 信号是否属于“车辆控制指令”）**

答：《安全指引》第二部分“重要数据判定”明确，控制指令包括“用于远程控制车门开关、车辆启动、转向、加速、制动、泊车和充放电控制、温度控制等电池管理的相关指令，不包含近场控制”，题目中提及的指令为车辆内部指令，非远程控制指令，不属于重要数据。

**43.近场蓝牙控制产生的车辆控制指令，是否为重要数据？**

答：《安全指引》第二部分“重要数据判定”明确，控制指令包

括“用于远程控制车门开关、车辆启动、转向、加速、制动、泊车和充放电控制、温度控制等电池管理的相关指令，不包含近场控制”，蓝牙属于近场通信协议，手机通过蓝牙发送的车辆控制指令，不属于重要数据。

**44.针对“控制指令”，若远程启动空调、远程开窗等需同时启动车辆，该指令是否为重要数据？**

答：《安全指引》第二部分“重要数据判定”明确，控制指令包括“用于远程控制车门开关、车辆启动、转向、加速、制动、泊车和充放电控制、温度控制等电池管理的相关指令，不包含近场控制”，题目中提及的场景中，远程启动空调、远程开窗等远程控制指令同时启动了车辆，相当于组合成了一条指令，应当按照相关判定规则进行重要数据判定。

**45.如何理解“其他情形”？**

答：汽车行业具有产业链长、业务场景多、发展速度快的特点，《安全指引》结合产业现状和实际需求，归纳总结了企业普遍存在、涉及数据出境较多的五类场景。但考虑到随着汽车产业新业务、新技术的快速迭代更新，新的数据出境场景必将不断涌现，因此增加“其他情形”用于补充。一是“其他出境业务场景中符合上述判定规则的”，适用于未在《安全指引》中给出的五类场景，但符合数据类型、数据项说明的，如符合相关的判定规则，则属于重要数据。二是汽车数据处理者按照国家有关规定和行业标准规范识别、申报重要数据，工业和信息化部、国家互联网信息办公室等相关部门公开或告知属于重要数据的。

### **三、数据出境流程类**

**46.汽车数据处理者如何开展重要数据目录备案？**

答：汽车数据处理者对数据进行定期梳理，按照《安全指引》第二部分“重要数据判定”，识别重要数据并形成本单位的具体目录；按照要求填写重要数据目录备案表，向本地区通信管理局备案。汽车数据处理者还应对重要数据目录进行定期维护、动态更新，备案内容

发生重大变化的，应当在发生变化的三个月内履行备案变更手续。

#### 47.汽车数据处理者如何申报数据出境评估？

答：汽车数据处理者应按照《数据出境安全评估办法》《促进和规范数据跨境流动规定》《数据出境安全评估申报指南（第三版）》等规定申报评估。

##### （1）明确申报主体

汽车数据处理者应通过境内法人主体申报数据出境安全评估；境内无法人主体的，应由境内分支机构申报；境内多家子公司如同属一家集团公司（母公司）且数据出境业务场景相似，可由集团公司（母公司）作为申报主体合并申报。汽车数据处理者不得采取数量拆分等方式，将依法应当通过安全评估的数据通过订立标准合同等方式向境外提供。

##### （2）梳理出境活动整体情况

收集本企业及境外接收方等相关方材料，梳理出境活动整体情况，包括：

1) 汽车数据处理者基本情况，包括股权结构、实际控制人、境内外投资情况等；

2) 汽车数据处理者拟出境数据情况，包括：

a.数据出境场景涉及业务、数据资产等情况；

b.数据出境的目的、范围、方式；

c.出境数据项情况，并以列表形式呈现；

d.拟出境数据在境内存储的系统平台、数据中心（包含云服务）等情况，数据出境链路相关情况，计划出境后存储的系统平台、数据中心等；

e.数据出境后向境外其他接收方提供的情况；

f.涉及个人信息的，按照自然人（去重）统计当年的出境数量，预估未来3年的出境数量。

3) 汽车数据处理者安全保障能力情况，包括数据安全能力、技术能力、数据安全保障措施有效性证明、遵守数据和网络安全相关法律法规的情况；

4) 境外接收方情况, 包括境外接收方基本情况, 境外接收方处理数据的用途、方式, 境外接收方履行责任义务的管理和技术措施、能力等;

5) 与境外接收方以法律文件形式约定出境数据情况, 明确双方责任义务, 具体内容包括:

a. 数据出境的目的、方式和数据范围, 境外接收方处理数据的用途、方式等;

b. 数据在境外保存地点、期限, 以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施;

c. 对于境外接收方将出境数据再转移给其他组织、个人的约束性要求;

d. 境外接收方在实际控制权或者经营范围发生实质性变化, 或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化, 以及发生其他不可抗力情形, 导致难以保障数据安全时, 应当采取的安全措施;

e. 违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式;

f. 出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用时, 妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

6) 汽车数据处理者认为需要说明的其他情况。

### (3) 开展自评估

#### 1) 自评估事项

汽车数据处理者应结合数据出境活动整体情况和相关材料重点评估以下事项:

a. 数据出境和境外接收方处理数据的目的、范围、方式等是否具有合法性、正当性、必要性;

b. 出境数据的规模、范围、种类、敏感程度, 数据出境是否会对国家安全、公共利益、个人或者组织合法权益带来风险;

c. 境外接收方承诺承担的责任义务, 以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全;

d.数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

e.与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等是否充分约定了数据安全保护责任义务；

f.其他可能影响数据出境安全的事项。

## 2) 发现问题并整改

汽车数据处理者在开展数据出境安全自评估过程中发现存在影响数据出境的风险和问题的，应及时整改，并记录相关情况。

## 3) 形成自评估结论

汽车数据处理者综合风险自评估情况和相应整改情况，对拟申报的数据出境活动作出客观的风险自评估结论，并充分说明理由。

## 4) 编制自评估报告

汽车数据处理者整理自评估工作情况、出境活动整体情况、出境活动的风险自评估情况及结论，编制形成数据出境风险自评估报告，并附相关证明材料。

### (4) 评估申报

#### 1) 准备申报材料

汽车数据处理者按照相关规定准备申报材料，包括：

a.统一社会信用代码证件影印件；

b.法定代表人身份证件影印件；

c.经办人身份证件影印件；

d.经办人授权委托书；

e.数据出境安全评估申报书；

f.与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件；

g.数据出境风险自评估报告；

h.其他相关证明材料。

汽车数据处理者需对所提交材料的真实性负责，提交虚假材料的，按照评估不通过处理，并依法追究相应法律责任。

#### 2) 确定申报方式

关键信息基础设施运营者以外的汽车数据处理者申报数据出境安全评估一般适用线上申报，关键信息基础设施运营者或者其他不适合通过线上系统申报数据出境安全评估的，采取线下申报流程。

### 3) 评估材料提交

汽车数据处理者按国家有关规定，向网信部门申报数据出境安全评估，并按要求补充或修改材料。

### (5) 评估结果确认

汽车数据处理者按照数据出境安全管理相关法律法规和评估结果通知书的有关要求，规范开展数据出境活动；

对评估结果有异议的，可以在收到评估结果通知书 15 个工作日内向网信部门申请复评。

### (6) 重新申报评估

出现以下情形之一的，汽车数据处理者应重新申报数据出境安全评估：

1) 向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的；

2) 延长个人信息和重要数据境外保存期限的；

3) 境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力影响出境数据安全的；

4) 汽车数据处理者或者境外接收方实际控制权发生变化影响出境数据安全的；

5) 汽车数据处理者与境外接收方法律文件变更等影响出境数据安全的；

6) 数据出境安全评估结果有效期届满仍需继续开展数据出境活动，但不满足评估结果延长条件的；

7) 已经通过评估的数据出境活动在实际处理过程中因不再符合数据出境安全管理要求被终止，汽车数据处理者在按照有关要求整改后，需要继续开展数据出境活动的；

8) 出现影响出境数据安全的其他情形。

## 48. 订立个人信息出境标准合同的流程是什么？

汽车数据处理者应按照《个人信息出境标准合同办法》《个人信息出境标准合同备案指南（第二版）》规定，订立个人信息出境标准合同。

#### （1）梳理出境活动整体情况

收集本企业及境外接收方等相关方材料，梳理出境活动整体情况，包括：

1) 汽车数据处理者基本情况，包括股权结构、实际控制人、境内外投资情况、组织架构和个人信息保护机构信息、整体业务与处理个人信息情况等；

2) 拟出境个人信息情况，包括：

a.个人信息出境涉及业务、个人信息收集使用、信息系统等情况；

b.汽车数据处理者和境外接收方处理个人信息的目的、范围、方式；

c.出境个人信息的规模、范围、种类、敏感程度，处理敏感个人信息情况；

d.拟出境个人信息在境内存储的系统平台、数据中心等情况，个人信息出境链路相关情况，计划出境后存储的系统平台、数据中心等；

e.个人信息出境后向境外其他接收方提供的情况。

3) 境外接收方情况，包括境外接收方基本情况，境外接收方处理个人信息的用途、方式，境外接收方履行责任义务的管理和技术措施、能力等；

4) 汽车数据处理者认为需要说明的其他情况。

#### （2）开展个人信息保护影响评估

##### 1) 评估事项

汽车数据处理者应结合个人信息出境活动整体情况和相关材料重点评估以下事项，包括：

a.个人信息出境和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性；

b.出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对国家安全、公共利益、个人信息权益带来的风险；

c.境外接收方承诺承担的义务，以及履行义务的管理和技术措施、

能力等能否保障出境个人信息的安全；

d.个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

e.境外接收方所在国家或者地区的个人信息保护政策和法规对标准合同履行的影响；

f.其他可能影响个人信息出境安全的事项。

## 2) 发现问题并整改

汽车数据处理者在开展个人信息保护影响评估过程中发现存在影响个人信息出境的风险和问题的，应及时整改，并记录相关情况。

## 3) 形成个人信息保护影响评估结论

汽车数据处理者综合个人信息保护影响情况和相应整改情况，对个人信息出境活动作出客观的影响评估结论，并充分说明理由。

## 4) 编制个人信息保护影响评估报告

汽车数据处理者整理个人信息保护影响评估工作情况、出境活动整体情况、出境活动的风险评估情况及结论，编制形成个人信息保护影响评估报告。

### (3) 签订合同

汽车数据处理者与境外接收方签订个人信息出境标准合同，标准合同生效后方可开展个人信息出境活动。

### (4) 备案

#### 1) 材料提交

汽车数据处理者按国家有关规定，向网信部门提交统一社会信用代码证件影印件、法定代表人身份证件影印件、经办人身份证件影印件、经办人授权委托书、承诺书、《个人信息出境标准合同》《个人信息保护影响评估报告》等备案材料。并按要求提交补充完善材料。

#### 2) 结果反馈

备案材料符合要求的，汽车数据处理者将获得备案编号；如需补充完善，汽车数据处理者应当在10个工作日内提交补充完善材料；逾期未补充完善的，本次备案程序将被终止。

### (5) 补充或重新备案

在标准合同有效期内出现下列情形之一的，汽车数据处理者应当

重新开展个人信息保护影响评估，补充或者重新订立标准合同，并履行相应备案手续：

- 1) 向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化的；
- 2) 延长个人信息境外保存期限的；
- 3) 境外接收方所在国家或者地区的个人信息保护政策和法规发生变化等可能影响个人信息权益的；
- 4) 可能影响个人信息权益的其他情形。

#### 49.汽车数据处理者如何开展个人信息出境认证？

答：汽车数据处理者应按照《个人信息出境认证办法》规定，开展个人信息出境认证。

##### (1) 认证申请

汽车数据处理者梳理出境活动整体情况、开展个人信息保护影响评估，向具备资质的专业认证机构申请认证。

##### (2) 配合认证

汽车数据处理者配合专业认证机构，按照认证基本规范、个人信息保护认证规则开展认证。

##### (3) 取得认证证书

通过认证后，汽车数据处理者取得认证证书，专业认证机构向全国认证认可信息公共服务平台报送证书相关信息。认证证书有效期为3年。证书到期需继续使用的，汽车数据处理者应当在有效期届满前6个月提出认证申请。

### 四、安全保护类

#### 50.汽车数据处理者如何开展汽车数据出境安全保护？

答：涉及汽车数据出境业务的，在落实汽车数据全生命周期安全保护基础上，还应按照《安全指引》第四部分“汽车数据出境安全保护要求”，从四个方面开展数据出境安全保护：

(1) **管理要求**。包括部门要求、人员要求、制度要求和审批要求。如：健全数据安全制度体系，明确数据出境安全保护要求；明确

由汽车数据出境安全管理部门负责组织开展数据出境安全评估申报、应急响应实施、境外接收方能力评估、出境安全审计等；明确汽车数据出境安全负责人由具备跨部门协调和资源调配能力的人员承担；建立汽车数据出境内部审批机制，确保汽车数据出境活动内部留痕。

**(2) 防护技术要求。**包括数据出境传输安全、数据出境安全监测、技术检查支撑等要求。如：采用校验技术、密码技术、安全传输通道或者安全传输协议等措施，防止汽车数据出境传输过程中被非授权访问和篡改；对出境相关的互联网出口流量进行实时监测，识别发现数据接收方 IP 地址异常、传输数据超范围等行为，按照 GB/T 《车联网安全管理接口规范》，形成安全告警日志并留存；对数据出境网络通信流量进行全量、抽样留存，并支持数据防篡改和内容解析。

**(3) 日志要求。**包括日志记录、日志留存、日志审计等要求。如：对数据出境相关的网络通信、主机操作等行为进行记录，形成网络流量日志和操作行为日志；对通信日志、操作行为日志、安全告警日志的访问和操作进行权限控制和审计，防止被非授权访问和篡改，日志留存时间不少于 3 年。

**(4) 应急处置要求。**建立数据违规出境处置能力，发现数据接收方 IP 地址异常、传输数据超范围等异常行为及时采取中断操作，对存在风险隐患的环节进行加固防护；详细记录安全事件信息以及相关攻击方式、安全事件报告等，处置完成后在规定时间内形成总结报告，按要求向相关主管部门报告数据安全事件处置情况。

**51.涉及一般数据出境的，是否也需要按照《安全指引》开展出境安全保护。**

答：《安全指引》第一部分“总则”明确，“汽车数据是指汽车设计、生产、销售、使用、运维等过程中涉及的个人信息和重要数据”，不包括一般数据。涉及一般数据出境的，企业应按照《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《汽车数据安全管理办法（试行）》《关于加强车联网网络和数据安全工作的通知》《工业和信息化领域数据管理办法（试行）》等法律法规政策文件要求，落实数据全生命周期安全保护，保障数据出境安全。

52.汽车数据处理者违反《安全指引》相关要求，是否存在相关法律责任？

答：汽车数据处理者违反《安全指引》相关规定的，依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全条例》等法律法规，结合具体违法情形依法予以相应处罚。