背景：

公有云越来越成为企业节省费用、提高服务能力、提高服务可用性的要求，越来越多的企业把用户数据、业务数据、运行数据部署在公有云上。

2021年6月，全国人民代表大会常务委员会通过了《中华人民共和国数据安全法》（以下简称《数据安全法》），并将于2021年9月1日起施行，从法律层面为数据安全提供了保障。《数据安全法》的出台，让数据合规和网络安全、大数据、云计算、公有云等话题又引起大众的新一轮讨论。

当《个人信息保护法》和《数据安全法》正式出台后，人们对于个人信息数据和个人隐私保护的法律问题会有更全面的认识和更高的要求。

观点和建议：

1. 数据安全法意味着什么？

答： 数据安全法的出台，意味着中国政府正式从立法层面对数据安全开展国家层面的管控和要求，任何组织、个人对数据的生命周期有了法律依据，满足数据安全合规要求是组织、个人、企业在运营过程中必须坚持和坚守的法律法规底线。

1. 企业上公有云的步伐、节奏是否会减慢？

答： 前期会存在这种现象，因为公用云在合规方面、数据安全管理、数据安全控制、数据安全技术等方面还需要一段时间去整改、提升、以满足法律法规要求和监管要求。 后期随着公有云服务商逐步的整改到位，数据安全能力的提升和合规要求的满足，企业、组织、个人对公有云的安全服务能力、安全管理能力、安全合规能力，尤其是数据安全保护能力方面的信任度会得到极大的提升，企业、组织、个人更放心地把业务、数据、信息部署在公有云上。

1. 企业需要关注什么

答： 企业更需要遵守中华人民共和国的相关法律法规，对用户信息、个人信息保护方面，隐私保护方面需要更高层的支持、需要更多的投入和技术支持，尤其是需要加强对数据安全颗粒度、细化程度的安全保护和能力支持，以前的把数据库当黑盒子整体保护、个人信息泄露等行为已经不大适合。

1. 企业需要做什么

答： 根据《数据安全法》、《个人信息保护法》、《网络安全法的》相关要求， 企业应当立即开展以下几个重点工作

4.1 成立专职的数据安全组织、个人信息保护组织，对相关的管理组织架构进行适当的调整，并确定各岗位层级的相关部门和责任人，形成一个团队管理层、执行层、协助层各岗位层级的合规职责，并将控制措施和技术工具融入企业现有管理流程中，优化现有管理流程、维护数据安全、有效利用数据。以前的兼职性质的组织可能存在风险。

4.2 授权专职数据管理者（DPO）、授权专职的个人信息安全负责人，以前的一人岗、一人多职有可能存在风险。

4.2 建立企业数据安全管理制度、提升相应的技术措施、基础措施、管理措施,可以基于网络安全法、数据安全法、等级保护条例、个人信息保护开展自评工作

4.3 开展数据分级分类工作，根据分类结果采取相应的措施，如技术上的提升（数据隔离、数据分离存储、权限控制、数据加密、去标识化、脱敏等），管理上的提升（发布管理制度、安排专职人员、安全培训等）

4.4 针对包含大量个人信息、重要数据的业务系统采取相应的措施，如技术上的提升（网络分区隔离保护、数据分离存储，加强权限控制），管理上的提升（发布管理制度、安排专职数据管理者、开展等级保护测评、备案）

4.5 识别核心数据和重要数据、根据国家要求识别关基数据和重要数据，识别数据跨境业务、跨境场景，做好备案申报，做好数据跨境监督，定期开展审计和自查，必要时邀请监管部门、主管机构进行监督检查。

4.6 加强对供应商、服务商（包括公有云）在安全管理能力、安全技术能力、安全合规遵循、管理制度、数据保护、隐私保护等方面的审核和监督检查，必要时针对相关服务合同进行修订和约束。

4.7 建立监测、预警机制，结合技术、工具进行数据行为的实时监测和预警处置（包括对应的流程、技术、工具、权限、管理框架），

4.8 做好数据安全事件风险防范措施和预案，重点需考虑如何应对投诉和监管的调查，根据职责和责任人的划分，分工配合提前做好应对措施，以避免损失和责任的进一步扩大

4.9 建立信息安全事件应急响应机制、数据上报机制，根据职责和责任人的划分，分工配合提前做好应对措施

1. 车企的影响

对车企（主机厂商）来说，重要数据主要包括如经管数据、营销数据、投资数据、生产数据、研发数据、财务数据、市场数据等；个人信息主要包括车主信息、潜客信息、经销商信息、用户车辆维修保养信息、用户服务信息、车主轨迹信息、车主导航信息、车主行为信息、车内录音录像等信息。

上述信息大量存放于内部或外部系统，对个人信息方面，主机厂商较多倾向于部署在外部公用云平台，以利用公有云的高可用性和高弹性接入能力、高性能计算能力。

上述个人信息大量被使用于服务推广、广告、营销、大数据分析、用户画像分析、用户行为分析、用户轨迹分析、用户服务提升等场景，存在个人信息泄露、个人信息转移、个人信息转让、个人信息买卖、大数据杀熟、用户行为泄露、用户行踪轨迹泄露等风险。依据《数据安全法》和《个人信息保护法》的相关要求，上述行为、风险均为违规，严重者甚至可能触发法律。

1. 车企应该做什么

车企（主机）厂商 建议尽快且必要开展以下工作

6.1 、识别上述个人信息存放的系统、设备、平台、业务流程、业务模块、权限

6.2 从架构上改进数据生命周期的管理过程，如搜集、存放、传输、使用等，尽量把个人信息相关数据，以技术手段+管理手段进行约束和规定，并尽量保存在企业内部IT环境

6.3 在未确定外部服务商、外部供应商符合、满足合规要求的情况下先行暂停（必要时终止）服务商、供应商的服务资格及服务能力，同时组建合格、合规的服务团队、支持团队

6.4 在未确定外部服务商、外部供应商符合、满足合规要求的情况下先行暂停（必要时终止）服务商、供应商的服务，在未能确认满足合规要求的情况下，尽量先把系统、数据、业务内迁，以规避短期风险

6.5 积极寻求高层支持，投入必要的资源（权限、组织、人员、技术、设备、系统、工具等），针对高风险进行整改  
6.6 与业务部门、合规部门、法务部门合作， 尽快寻求合适、合规的外部服务商、供应商，开展自查、自评估、自整改工作，在短期内规避、解决高风险事项

6.7 建立长期作战思维，建立持续数据安全保护能力、个人信息保护能力，并持之以恒地执行下去。

结语：

中华人民共和国基于国家安全要求，陆续出台了《网络安全法》、《数据安全法》、《个人信息保护法》，从国家立法层面、国家安全高度提出了整体要求。

对车企（主机厂商），相关行业监管机构也陆续出台了一系列关于车辆安全、车辆行驶安全、智能网联车安全、车联网安全等方面的法律法规和相关要求。

行车安全是关系到人员安全、人生安全、财产安全的重要支撑点，车企（主机厂商）更需要严密关注、积极采取措施，在行业监管机构、行业部门的驱动和带领下，认真、负责、积极、主动地开展自查、自评估、自整改等工作，虽任重道远，车企应当仁不让，积极拥抱、遵循法律法规的要求，以人员安全、人生安全、财产安全为最高目标。

附录1：实践指南

# 组织建设

组织机构应该在条件允许的情况下设立数据安全管理部门并招募相关的管理人员和技术人员，

* 负责为公司提供必要的技术支持
* 对数据业务设计开发等阶段开展数据安全管理工作
* 为组织机构制定整体的有效的数据安全管理文档以及规范化表达，
* 为组织机构建立数据安全管理制定流程和审评机制
* 对组织机构内部的数据安全管理的制定场景进行风险评估
* 为技术人员建立数据业务安全需求分析系统，确保任何针对需求分析文档的操作都会被记录都可以追踪溯源
* 为技术人员进行专门的安全意识培训，并推动以上相关要求在组织机构中确实可靠的落地执行

# 人员能力

# 管理人员

* 必须具备良好的数据安全风险意识，熟悉国家网络安全法律法规以及组织机构所属行业的政策和监管要求
* 在进行数据安全管理管理以及制定相应的数据安全管理流程和评审机制的时候，严格按照《网络安全法》、《数据安全法》、《个人信息保护法》等国家相关法律法规和行业规范执行
* 相关的管理人员具备一定的数据安全管理管理经验，拥有良好的数据安全管理管理专业知识基础且通过了岗位能力测试
* 熟悉主流的数据安全管理管理制度、管理流程、管理要求和技术工具，能够根据不同的管理要求和数据安全管理场景进行相应的风险评估
* 能够根据数据安全管理管理和审核的整体需求明确应该使用的数据安全管理管理工具。
* 能够主动根据行业及政策变化更新相关的知识和技能，具备能够结合业界标准、合规准则、业务场景制定数据安全管理管理制度的能力。

# 技术人员

* 同样也必须具备良好的数据安全风险意识，熟悉相关的法律法规以及政策要求，熟悉主流厂商的数据安全管理挖掘案例
* 熟悉主流的数据安全管理工具及其使用方法
* 熟悉相关的数据安全管理的技术知识，拥有至少一年以上的数据安全管理挖掘经验
* 充分理解并执行由管理人员制定的数据安全管理管理制度，能够依据国家法律法规标准等分析数据安全合规性需求
* 能够结合组织机构的战略规划、数据服务业务目标和业务特点明确数据服务安全需求和安全规划实施的优先级，
* 能够主动根据政策变化和技术发展更新自身相关知识和技能的能力，
* 能够对突发的事件进行应急处理的能力

# 落地执行性确认

针对数据安全管理管理岗位人员能力的实际落地执行性确认，可通过内部审计、外部审计等形式以调研访谈、问卷调查、流程观察、文件调阅、技术检测等多种方式实现。

# 制度流程

# 需求分析管理目的

通过建立针对组织业务的数据安全管理体系，分析组织内数据业务的安全需求，确保核心数据与资源的保密性、完整性和可用性。

# 需求分析管理规范

组织机构需根据《网络安全法》、《数据安全法》、《个人信息保护法》等国家相关法律法规和行业规范

* 建立数据安全管理制定流程和审评机制
* 制定数据安全管理文档以及规范化表达，保证需求分析的各个阶段能够有序、可控的进行
* 建立数据业务安全需求分析系统，对所有的数据业务的需求分析的申请、需求分析以及相关安全方案进行记录
* 保证对所有的数据业务的安全需求分析过程的有效追溯