**金融科技时代数据安全治理问题与建议**

随着金融科技的迅猛发展，数据已经成为了金融服务行业中不可或缺的资源。但是，随之而来的数据泄露、信息安全、身份诈骗等问题也越来越受到关注。因此，在金融科技时代，必须加强数据安全治理，保障金融科技的可持续发展。

一、数据安全风险

数据安全风险指的是数据泄露、丢失或被盗用等安全事件对金融行业造成的潜在威胁。在金融科技时代，数据安全风险十分严峻，其表现在以下几个方面：

1. 大规模数据滥用：金融科技平台储存大量用户信息，如不加以合理的利用会直接导致个人隐私和数据漏洞大幅度增加，进而导致数据滥用问题，如用户信息泄露、诈骗等。

2. 数据交换不透明：数据交换不透明将会导致数据的源流向追溯、数据所有权与责任认定出现问题，进而导致数据交易中存在的风险变得不可预估。

3. 数据资产意识缺失: 部分金融科技企业未能充分认识到数据的价值与风险性质，未能把数据作为重要的资产进行管理。

4. 数据隐私保护问题: 随着金融科技业务的发展，以国家标准、行业标准为基础的数据隐私保护手段不应再是当前重要的问题，国家和行业应加强对该方面的监管和管理。

二、加强数据安全治理

对于金融科技企业来说，要想解决数据安全风险，必须从以下几个方面加强数据安全治理:

1. 制定数据安全管理规范: 对于数据的获取、存储、共享、传输、使用、销毁等全过程制定严格的数据安全管理规范，明确数据的安全渠道、权限控制、数据仓库搭建等方面的标准。

2. 建立数据汇集风险评估机制: 通过风险评估机制，对于金融科技企业的数据资产进行梳理、评估，以此厘清数据资产价值和风险，为数据使用方提供更好的数据评估工具。

3. 完善数据隐私保护制度：要求金融科技企业完备的隐私保护措施，加强对数据隐私泄露等现象，并加强对泄露行为的惩治，以此加强数据隐私保护机制。

4. 提高员工数据安全意识：利用各种形式的宣传教育，提高员工数据安全意识。如制定内部数据管理规范，加强工作人员的技能培训，加强安全意识培养，提高信息保密意识等。

5. 强化数据社会责任意识：金融科技企业应当树立更加严谨、规范的管理意识，培养责任感和社会良知，加强人民群众对数据安全的居民感，努力提高金融科技行业的社会责任感和形象。

6. 加强数据监管和审查：政府应成立数据隐私和信息保护委员会，强化对金融科技行业的监管和审查，预防和治理金融网络犯罪，完善金融行业的信息保护和风险控制机制。

三、结语

在金融科技时代，数据安全治理问题显得尤为重要。针对上述数据安全风险，金融科技企业必须积极加强数据安全治理，提升信息保护意识，制定严格的数据安全管理规范，在保障个人隐私和数据安全的基础上，推动金融业向智能金融方向迈进。