

个人信息安全保护

公开课小课堂



主讲：曹阳

时间：2021年9月



课程目录

01

标准制定背景
个人信息保护原则

02

数据来源的合法基础

03

数据保留与使用
数据对外提供

04

特殊类型的和儿童的个人信息

05

供应商管理

06

数据主体的权利
数据安全保护

07

数据境外提供
数据泄露与数据安全事件响应

第七课 数据境外提供、数据泄露与数据安全事件响应

数据境外提供的条件

研究服务提供者因市场研究需要，需确向境外提供个人信息的，应当至少具备下列一项条件：

- ↗ 依照相关法律规定通过国家网信部门组织的安全评估；
- ↗ 按照国家网信部门的规定经专业机构进行个人信息保护认证；
- ↗ 与境外接收方订立合同，约定双方的权利义务，并监督其个人信息处理活动符合中华人民共和国境内法律、行政法规规定以及本标准规定的个人信息保护标准；
- ↗ 法律、行政法规或者国家网信部门规定的其他条件。

» 第七课 数据境外提供、数据泄露与数据安全事件响应

数据境外提供的条件

12.1.2 获得授权同意

个人信息出境，应向个人说明个人信息数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，并经其同意。未成年人个人信息出境须经其监护人同意。

第七课 数据境外提供、数据泄露与数据安全事件响应

数据境外提供的条件

完成出境安全评估

研究服务提供者在中华人民共和国境内运营中收集和产生的个人信息，应当在境内存储。因特定市场研究需要，确需向境外提供的，应当进行安全评估，并对评估结果负责。个人信息出境安全评估应重点评估以下内容：

- ✎ 个人信息出境的必要性，以及是否符合法律、行政法规的规定；
- ✎ 涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及个人是否同意其个人信息出境等；
- ✎ 个人信息接收方是否有损害个人合法权益的历史、是否发生过重大安全事件；
- ✎ 个人信息接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等；
- ✎ 个人信息出境及再转移后被泄露、毁损、篡改、滥用等风险；
- ✎ 个人信息出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险；
- ✎ 其他需要评估的重要事项。

» 第七课 数据境外提供、数据泄露与数据安全事件响应

禁止出境的情况

存在以下情况之一的，个人信息不得出境：

- ↗ 个人信息出境未经受访者或其他个人同意，或可能侵害个人利益；
- ↗ 个人信息出境可能给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益；
- ↗ 其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。

第七课 数据境外提供、数据泄露与数据安全事件响应



因5亿用户数据泄露问题 新浪微博被工信部约谈

据工信部官网3月24日消息，3月21日，针对媒体报道的新浪微博因用户查询接口被恶意调用导致App数据泄露问题，工业和信息化部网络安全管理局对新浪微博相关负责人进行了问询约谈。据悉，工信部要求新浪微博按照《网络安全法》《电信和互联网用户个人信息保护规定》等法律法规要求，对照工信部等四部门制定的《App违法违规收集使用个人信息行为认定方法》，进一步采取有效措施，消除数据安全隐患。具体要求有：一是要尽快完善隐私政策，规范用户个人信息收集使用行为；二是要加强用户信息分类分级保护，强化用户查询接口风险控制等安全保护策略；三是要加强企业内部数据安全，定期及新业务上线前要开展数据安全合规性自评估，及时防范数据安全风险；四是要在发生重大数据安全事件时，及时告知用户并向主管部门报告。对此，新浪微博回应称，公司高度重视数据安全



我从黑市人肉出34.6万条个人信息，多数受害者麻木不仁

原创 点击右边星标 一条 2019-09-11



据中国互联网网络信息中心的数据，截至2018年底，中国的手机网民8.17亿。我们每个人的日常生活，已经与互联网牢牢捆绑在了一起。手机支付、人脸识别、定位分享……我们在享受这些便利的时候，同时也面临着一场不小的隐私危机。



因为ZAO，陌陌被工信部约谈……

商周君 商业周刊中文版 2019-09-04



9月3日，针对媒体公开报道和用户曝光的“ZAO”App用户隐私协议不规范，存在数据泄露风险等网络数据安全问题，工业和信息化部网络安全管理局对北京陌陌科技有限公司相关负责人进行了问询约谈，要求其严格按照国家法律法规以及相关主管部门要求，组织开展自查整改，依法依规收集使用用户个人信息，规范协议条款，强化网络数据和用户个人信息安全保护。同时，要进一步加强新技术新业务安全评估，切实采取有效措施，积极防范自有业务平台被利用实施电信网络诈骗等风险隐患。

第七课 数据境外提供、数据泄露与数据安全事件响应

数据泄露 事件分类

01

保密性泄露：个人信息数据在未经授权或意外的情况下被披露或取用；

02

完整性泄露：个人数据在未经授权或意外的情况下被更改；

03

可用性泄露：个人数据意外或未经授权的丢失或被破坏。

第七课 数据境外提供、数据泄露与数据安全事件响应

个人信息安全事件应急处置和报告

安全事件应急预案

研究服务提供者应制定个人信息安全事件应急预案，同时应定期（至少每年一次）组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程。

安全事件应急处置

发生个人信息安全事件后，研究服务提供者应根据应急响应预案进行以下处置：

- 记录安全事件内容，包括但不限于：发现安全事件的人员、时间、地点，涉及的个人信息及人数，发生安全事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门；
- 评估安全事件可能造成的影响，并采取必要措施处理事态，消除隐患；
- 按照《国家网络安全事件应急预案》等有关规定及时上报，报告内容包括但不限于：涉及个人的类型、数量、内容、性质等总体情况，安全事件可能造成的影响，已采取或将要采取的处置措施，安全事件处置相关人员的联系方式；
- 个人信息泄露安全事件可能会给个人的合法权益造成严重危害的，如个人敏感信息的泄露，按照13.2的要求实施安全事件的告知。
- 根据相关法律法规变化情况，以及安全事件处置情况，及时更新应急预案。

第七课 数据境外提供、数据泄露与数据安全事件响应

安全事件告知

安全事件告知要求

研究服务提供者应及时将安全事件相关情况以邮件、信函、电话、推送通知等方式任选其一告知受影响的个人。难以逐一告知个人时，应采取合理、有效的方式发布与公众有关的警示信息。

安全事件告知内容

安全事件告知内容应包括但不限于：

- ✎ 安全事件的内容和影响；
- ✎ 已采取或将要采取的处置措施；
- ✎ 个人自主防范和降低风险的建议；
- ✎ 针对个人提供的补救措施；
- ✎ 个人信息保护负责人和个人信息保护工作机构的联系方式。

谢谢!



主讲：曹阳

时间：2021年9月

