员工数据安全保密培训

曾咏梅　合伙人
国浩律师（海南）事务所

目 录

CONTENTS

商业秘密基础知识

- 商业秘密
- 侵犯商业秘密的行为
- 立法保护
- 侵犯商业秘密的法律责任

商业秘密

1.概念

指不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。

商业秘密往往按重要程度由高到低划分为：“绝密级”、“机密级”、“秘密级”。

2.表现形式

产品配方、制作工艺、产销策略、客户名单、供货渠道、尚未公布的重大合同、重大资产置换方案等。

有下列情形之一的，人民法院可以认定有关信息为公众所知悉

（一）该信息在所属领域属于**一般常识或者行业惯例**的；

（二）该信息仅涉及产品的尺寸、结构、材料、部件的简单组合等内容，所属领域的相关人员**通过观察上市产品即可直接获得**的；

（三）该信息已经在**公开出版物**或者其他媒体上公开披露的；

（四）该信息已通过公开的**报告会、展览**等方式公开的；

（五）所属领域的相关人员从其他**公开渠道**可以获得该信息的。

将为公众所知悉的信息进行整理、改进、加工后形成的新信息，符合本规定第三条规定的，应当认定该新信息不为公众所知悉。

具有下列情形之一，人民法院应当认定权利人采取了相应保密措施

（一）签订保密协议或者在合同中**约定保密义务**的；

（二）通过**章程、培训、规章制度、书面告知**等方式，对能够接触、获取商业秘密的员工、前员工、供应商、客户、来访者等提出保密要求的；

（三）对涉密的厂房、车间等生产经营场所**限制来访者**或者进行区分管理的；

（四）以标记、分类、隔离、加密、封存、限制能够接触或者获取的人员范围等方式，**对商业秘密及其载体进行区分和管理**的；

（五）对能够接触、获取商业秘密的计算机设备、电子设备、网络设备、存储设备、软件等，采取**禁止**或者**限制使用、访问、存储、复制**等措施的；

（六）要求**离职员工**登记、返还、清除、销毁其接触或者获取的商业秘密及其载体，继续承担保密义务的；

（七）采取其他合理保密措施的。

客户名单

商业秘密中的客户名单，一般是指客户的名称、地址、联系方式以及交易的习惯、意向、内容等构成的**区别于相关公知信息的特殊客户信息**，包括汇集众多客户的客户名册，以及保持长期稳定交易关系的特定客户。

客户基于对职工个人的信赖而与职工所在单位进行市场交易，该职工离职后，能够证明客户自愿选择与自己或者其新单位进行市场交易的，应当认定没有采用不正当手段，但职工与原单位另有约定的除外。

立法保护

国内立法

- 《中华人民共和国民法典》
- 《中华人民共和国反不正当竞争法》（2019修正）
- 《中华人民共和国刑法》
- 《最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定》
- 《最高人民法院关于审理不正当竞争民事案件应用法律若干问题的解释》

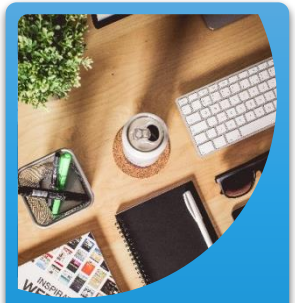
重要的国际公约

- 《与贸易有关的知识产权协议》（TRIPS）
- 《反不正当竞争法示范条款》

侵犯商业秘密的行为

直接非法获取

以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密；



间接非法使用

披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密；

违反约定情形

（教唆、引诱、帮助他人）违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密；

明知、应知情形

第三人明知或者应知商业秘密权利人的员工、前员工或者其他单位、个人实施本条第一款所列违法行为，仍获取、披露、使用或者允许他人使用该商业秘密的，视为侵犯商业秘密。

侵犯商业秘密的法律责任

民事法律责任	行政法律责任	刑事法律责任
主要有违约责任和侵权责任。其中，违约责任又分支付违约金和赔偿实际损失两种形式。 承担侵权责任方式有：停止侵害、排除妨碍、赔偿实际损失等。 以上实际损失应以权利人因遭受侵害所产生的直接损失额为准，如果权利人实际损失难以计算的，赔偿额为侵害人在侵害期间因侵害所获得的利润，并加上权利人因调查该侵害人侵害其合法权益的不正当竞争行为所支付的合理费用。	根据《反不正当竞争法》的有关规定：经营者以及其他自然人、法人和非法人组织违反本法第九条规定侵犯商业秘密的，由监督检查部门责令停止违法行为，没收违法所得，处**十万元以上一百万元以下的罚款**；情节严重的，处**五十万元以上五百万元以下**的罚款。	侵犯商业秘密罪 《刑法》第二百一十九条： 有下列侵犯商业秘密行为之一，给商业秘密的权利人造成重大损失的，**处三年以下有期徒刑或者拘役，并处或者单处罚金**；造成特别严重后果的，处**三年以上七年以下**有期徒刑，并处罚金。 （一）以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密的； （二）披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密的； （三）违反约定或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密的。 明知或者应知前款所列行为，获取、使用或者披露他人的商业秘密的，以侵犯商业秘密论。

数据安全基础知识

- 数据安全法重点制度

数据安全法重点制度

- 数据分类分级制度
- 重要数据保护制度
- 数据安全风险评估预警
- 数据审查和数据出境
- 数据安全保护义务
- 政务数据安全与开放

数据分类分级制度

《数据安全法》第二十一条：国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行**分类分级保护**。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。
各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据 进行重点保护

- 由国家建立数据分类分级保护制度
- 根据数据遭到篡改、破坏、泄露或非法获取、非法利用后造成的危害后果对数据进行分级分类；其中危害后果既包括对直接占有这部分数据的企业或者组织可能产生的危害，也包括对国家安全、公共利益或者公民、组织 合法权益造成的危害。

数据分类分级制度

数据分类分级制度的探索：

- 《工业数据分类分级指南（试行）》
- 《证券期货业数据分类分级指引》
- 《个人金融信息保护技术规范》

上述文件的主要规范对象是：**直接占有数据的企业或组织。**

- 主体：个人数据、企业数据和政府数据等。
- 技术：电子数据与系统环境数据等。
- 对“国家安全”的影响效果：“一旦泄露、破坏或者非法利用就严重危及国家安全的重要数据” 和除此以外的 “一般数据”。

重要数据保护制度

《数据安全法》第二十一条：国家数据安全工作协调机制 统筹协调有关部门制定重要数据目录，加强**对重要数据的保护。**

关系**国家安全、国民经济命脉、重要民生、重大公共利益等**数据属于**国家核心数据**，实行更加严格的管理制度。

- 《数据安全法》将数据分类分级保护制度与重要数据目录直接对应，并要求各地区、各部门按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，更具参考性和实操性，深化加强对重要数据的保护。



重要数据保护制度

什么是重要数据?

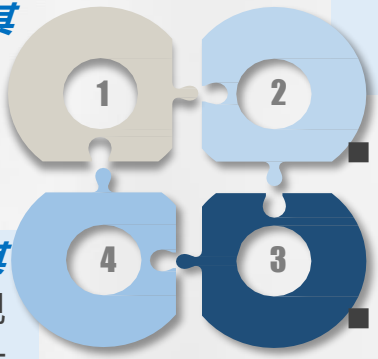
- 《数据安全法》并未明确界定什么是重要数据，但我们可以从其他法律法规中识别何为重要数据。
- 《个人信息和重要数据出境安全评估办法（征求意见稿）》第九条，对重要数据界定为：“重要数据，是指与***国家安全、经济发展，以及社会公共利益密切相关***的数据，具体范围参照国家有关标准和重要数据识别指南。”
- 《数据安全管理办法（征求意见稿）》，对“重要数据”界定为：“重要数据，是指一旦泄露可能直接影响***国家安全、经济安全、社会稳定、公共健康和安全***的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等。重要数据一般不包括企业生产经营和内部管理信息、个人信息等。”
- 《数据出境安全评估指南（征求意见稿）》附录 A《重要数据识别指南》：重要数据是指相关组织、机构和个人在境内收集、产生的***不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据（包括原始数据和衍生数据）***：石油天然气、煤炭、石化、电力等27个行业及其他。
- 虽然上述征求意见稿并未生效，但具有一定的参考价值，可预先进行了解，做好重要数据保护措施。

数据安全保护义务

➢ *数据活动组织和个人的内部合规制度*

- 建立健全***全流程数据安全管理制度***；组织开展***数据安全教育培训***，采取相应的***技术措施和其他必要措施***，保障数据安全（第二十七条）。

- 采取合法、 正当的方式，不得***窃取或者以其他非法方式获取***数据；在法律、 行政法规规定的目的和范围内收集、 使用数据（第三十二条）。



- ***重要数据的处理者***应当明确数据安全负责人和管理机构，落实数据安全保护责任（第二十七条）。

- 开展数据处理活动应当***加强风险监测***，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施（第二十九条）；

- 重要数据的处理者应当按照规定对其数据处理活动***定期开展风险评估***，……包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等（第三十条）。

数据安全保护义务

➢ ***数据活动组织和个人的告知、报告、协助调查等义务***

- 发生***数据安全事件***时，应当按照规定及时***告知用户***并向***有关主管部门***报告（第二十九条）。
- 重要数据的处理者……定期开展风险评估，并向有关主管部门***报送风险评估报告***（第三十条）。
- ***公安机关、 国家安全机关***因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过***严格的批准手续***，依法进行，有关组织、 个人应当***予以配合***（第三十五条）。
- 非经中华人民共和国主管机关批准，境内的组织、个人***不得向外国司法或者执法机构***提供存储于中华人民共和国境内的数据。（第三十六条）。

防范措施与司法救济

企业建立商业秘密保护机制

1. 商业秘密管理
2. 对员工的教育
3. 防控来自外部的侵权行为

泄露商业秘密，分为“有意”和“无意”的不同情况，前者主要依靠“硬件”上的措施去预防，使用各种加密技术措施；后者主要依靠“软件”上的措施去预防，通过警示教育和文件流程管理，使员工有保密意识，在公司里建立适度的保密文化。

企业建立商业秘密保护机制

1. 商业秘密管理

（1）商业秘密分级、登记，加保密标识
（2）专员或部门管理、监控商业秘密
（3）用门禁、上锁、权限设置等方式控制涉密场所
（4）用密码等措施限制访问和拷贝含有商业秘密的文件（密码应当经常更换）
（5）商业秘密载体特殊管理，例如禁止含有商业秘密的电脑联网，禁止插入U盘等外部存储
（6）分层分段开发，使非核心员工仅能接触商业秘密片段
（7）携带涉密计算机和文件外出应当履行批准手续
（8）员工调岗、离职妥善交接商业秘密，必要时签订竞业限制协议
（9）界定职务发明、职务作品，避免商业秘密权属发生争议

企业建立商业秘密保护机制

2. 对员工的教育

员工如果没有保密意识，再完善的商业秘密管理制度也是摆设。

对员工的教育分两部分：

（1）对员工手册、保密制度的培训学习；
（2）对侵犯商业秘密的法律后果的了解。

企业建立商业秘密保护机制

3. 防控来自外部的侵权行为

（1）与合作公司签订保密协议
（2）限制外人访问涉密场所和商业秘密载体
（3）用技术手段（如加密）和物理手段（如断网）防范泄密
（4）委托开发合同明确约定技术成果的归属
（5）某些商业秘密中可插入特殊的甚至错误的字符、字段，便于日后举证（要视情况，不一定有用）

企业被侵犯商业秘密后的司法救济

1. 违约行为
2. 民事侵权行为
3.不正当竞争行为/犯罪行为

企业一旦发现商业秘密被泄露，应立即采取有效措施，比如可以根据民法典、反不正当竞争法、刑法的相关规定追究相关人员的责任，避免损失进一步扩大。

企业被侵犯商业秘密后的司法救济

1.从违约行为角度：

企业员工违反保密协议和竞业限制协议约定的保密义务，应按约定对企业损失承担相应的赔偿责任，对于已获得的收益应当返还企业。企业可以根据约定对相关人员提起民事诉讼。

企业被侵犯商业秘密后的司法救济

2.从民事侵权行为角度：

如果商业秘密被他人非法获取、泄露或使用，其权利人可依侵权行为法追究侵权人的侵权责任。《民事诉讼法》第一百条规定了保全制度：“人民法院对于可能因当事人一方的行为或者其他原因，使判决难以执行或者造成当事人其他损害的案件，根据对方当事人的申请，可以裁定对其财产进行保全、责令其作出一定行为或者禁止其作出一定行为;当事人没有提出申请的，人民法院在必要时也可以裁定采取保全措施。”

这样对于有关商业秘密的侵权行为，在诉讼中可以申请法院禁止侵权方做出侵权行为，从而保护企业的合法权利。

企业被侵犯商业秘密后的司法救济

3.从不正当竞争行为角度：

依反不正当竞争法追究其法律责任，其法律责任一般是刑事责任。企业遇到重大泄露商业秘密的行为，又无法查清泄密人员时，可以果断向公安机关报案。

04 公司商业秘密管理制度概览

全体员工对工作范围内所掌握的商业秘密，均负有保密的责任和义务

（一）不得刺探与本职工作或本身业务无关的商业秘密；

（二）不得向不承担保密义务的任何第三人披露公司的商业秘密；

（三）未经公司授权和许可不得出借、赠与、出租、转让公司商业秘密或协助不承担保密义务的任何第三人使用公司的商业秘密；

（四）如发现商业秘密泄露或者自身过失泄露商业秘密，应当采取有效措施防止泄密进一步扩大，并及时向本部门负责人或者知识产权与法务部报告；

（五）涉及商业秘密的资料需要进行传输时，应使用公司邮箱、设有权限的公共盘或其他公司指定的传输平台，禁止使用微信、QQ、SKYP、WhatsApp等一切即时通讯软件；

全体员工对工作范围内所掌握的商业秘密，均负有保密的责任和义务

（六）涉及商业秘密的载体（如纸质记录、电子储存设施等）应随时处于可监管的状态，当人员离开时，涉及商业秘密的载体应放置于上锁的或有权限控制的柜/抽屉中。

（七）应当使用密码等技术措施限制访问和拷贝含有商业秘密的文件，且密码需经常更换，密码的更换与保存由专（兼）职保密员负责管理。

员工与客户接洽注意事项

- 接入。员工接待客户进入工作场所，应全程陪同，严禁随意参观、拍照、记录等行为。
- 交流。员工在与客户进行交流时，仅谈及合作项目信息，不得谈及合作项目之外的其他涉密信息。当客户询问涉及公司秘密时，员工不知道如何作答时，需礼貌谢绝。员工与客户交流时，应维护公司形象，不得涉及公司管理制度及商业秘密等。
- 送回与客户接洽完毕，需将客户送出公司，不得任客户在工作场所随意出入、闲逛。

计算机安全管理和策略

- 员工在离开正在工作的计算机系统时，需要锁定屏幕；
- 员工在使用完计算机系统后，需要及时注销或者关闭计算机系统；
- 为了使系统安全设置有效，文件存储格式应采用NTFS文件格式，按照应用程序的要求分配用户的文件/文件夹许可权限；
- 禁用计算机系统的USB端口。未经信息技术部门授权，禁止使用可移动存储设备等外界设备；
- 设计保密项目的计算机系统，需要开启BitLocker加密。密钥需要存放在公共盘。

信息安全管理措施

- 各中心/部门需按照商业秘密的等级，在公司共享文件夹上设置工作相关的资料、文档、数据等工作文件夹，并设置符合商业秘密管理的访问权限。当人员岗位调动或者调整时，应按照新的岗位设定相关的访问权限，同时清除原有的权限设置。
- 各中心/部门应要求员工定期上传工作相关的电子资料、数据到合适的文件夹。
- 秘密等级高的文件在集团内部或者与客户之间流转，应当设置密码或者AD RMS权限控制，防止因工作失误造成的泄密。
- IT运维部应默认关闭计算机系统USB存储功能并禁止访问百度云网盘等云存储相关的网站。
- IT运维部应禁止访问如QQ邮箱等外部个人邮箱网站。
- 如无工作需要，IT运维部应禁止安装QQ、微信等个人即时通讯软件。

信息安全管理措施

- IT运维部应减少不受控的小打印机，员工打印应使用刷卡打印系统。
- IT运维部应启用上网行为管理，封禁工作无关的网站访问，并对研发相关员工的网络进行管理，启用黑白名单访问模式。
- IT运维部应加强计算机病毒、木马、勒索软件等防护，做好钓鱼、欺诈邮件的识别培训工作。
- IT运维部应按照NJ-IT-SOP-0003《电子数据备份和归档管理规程》，做好数据备份及归档相关工作，确保数据安全。归档的数据需要加密存储。
- 对笔记本电脑、研发相关的台式机，IT运维部应进行硬盘加密，确保设备失窃、丢失后的信息安全。
- 员工不得以任何借口将个人账户密码透露给他人。
- 员工离开电脑前，应及时将电脑屏幕锁定，并将设备置于上锁环境中。
- 因工作需要接触到集团商业秘密的外包人员、实习生或者供应商人员，应接受数据安全保密培训，并签署数据保密协议。

信息安全事件报告

- IT运维部应建立入侵检测和防御系统，以监测信息安全事件。
- 对于监测到的信息安全事件，IT运维部应及时通知信息归属部门。
- 如发生重要信息安全事件，IT运维部应负责调查事件原因，详细记录事件发生及处理经过。



员工离职信息安全注意事项

- 员工离职获批后，IT运维部应立即关闭所有信息管理系统的访问权限，共享文件夹的权限；
- 员工提出离职后，IT运维部应立即关闭手机邮箱、网页邮箱等移动访问公司电子邮件系统的权限。酌情保留笔记本电脑的使用权限。
- 对于总监级别及以上的员工或者设计秘密级高的核心员工，在离职申请批准后，IT运维部应立即禁用个人计算机账号。如有必要，内部审计部应对其工作资料进行离职审计。



THANKS FOR WATCHING

感谢您的认真观看

国浩律师事务所
曾咏梅　合伙人
Tel: 13813818001
E-mail: zengyongmei@grandall.com.cn
www.grandall.com.cn