

「案例精选」

适用《数据安全法》的行政处罚案例

01

「2022年」





案例1：瞒报行程轨迹信息，不配合公安机关进行数据调取被处罚

案例 瞒报行程轨迹信息，不配合公安机关进行数据调取被处罚

案由

2022年1月28日，违法行为人韦某乘坐飞机（航班号HU7375）从广东深圳直达广西百色巴马机场，后由韦某堂哥韦建锋开车到巴马机场接送韦某回到田阳区田州镇万和新城小区居住，公安民警向韦某了解情况时，韦某却瞒报行程轨迹信息，后被公安民警查实。根据《中华人民共和国数据安全法》第三十五条之规定，拟对违法行为人韦某处以罚款二百元的处罚。

处罚措施 根据《中华人民共和国数据安全法》第35条，拟对违法行为人韦某处以**罚款二百元**的处罚。



案例2：广州某公司开发的“驾培平台”未履行数据安全保护义务

案例 广州某公司开发的“驾培平台”未履行数据安全保护义务

案由

2022年2月，在开展广州民生实事“个人信息超范围采集整治治理”专项工作中，广州警方检查发现，广州某公司开发的“驾培平台”存储了驾校培训学员的姓名、身份证号、手机号、个人照片等信息1070万余条，但该公司没有建立数据安全管理制度和操作规程，对于日常经营活动采集到的驾校学员个人信息未采取去标识化和加密措施，系统存在未授权访问漏洞等严重数据安全隐患。系统平台一旦被不法分子突破窃取，将导致大量驾校学员个人信息泄露，给广大人民群众个人利益造成重大影响。

处罚措施

根据《中华人民共和国数据安全法》第27条，广州警方对该公司未履行数据安全保护义务的违法行为，依法处以**警告并处罚款人民币5万元**的行政处罚。



案例3：枣庄某公司存储个人信息至第三方云平台上，未履行数据安全保护义务

案例 枣庄某公司存储个人信息至第三方云平台上，未履行数据安全保护义务

案由

2022年5月，枣庄网警在执法检查中发现，某公司自建收费系统，通过公众号采集公民个人信息，存储在第三方云平台上，但对采集的数据未采取安全防护技术措施，未依法履行网络安全保护义务。

处罚措施

枣庄市台儿庄网警根据《中华人民共和国数据安全法》第27条第一款、第45条第一款，对该公司予以行政**警告处罚，并责令改正**。该案例也是山东省首起适用《中华人民共和国数据安全法》的行政处罚案件。



案例4：洛阳某公司数据在境外网站公开售卖，未保障数据安全被处罚

案例 洛阳某公司数据在境外网站公开售卖，未保障数据安全被处罚

案由

2022年7月，洛阳警方网安部门发现某公司数据在某境外网站被公开售卖后，立即对该公司进行了相关检查。

经查，该公司开展数据处理活动时，未依法建立健全全流程数据安全管理制度，未采取相应的技术措施和其他必要措施来保障数据安全，导致数据被泄漏。

处罚措施

根据《中华人民共和国数据安全法》第四十五条规定，该公司未按规定履行数据安全保护义务，存在重大网络安全隐患。最终，警方给予该公司**人民币5万元**的行政处罚，并对该公司主管负责人处**1万元的行政处罚**。



案例5：上海某科技公司在处理政务类数据时违规，未履行数据安全保护义务被处罚

案例 上海某科技公司在处理政务类数据时违规，未履行数据安全保护义务被处罚

案由

2022年10月，上海网信办发现，某科技公司在处理政务类数据时违规操作，且未采取相应的技术措施和其他必要措施保障数据安全，导致数据存在泄露风险。

处罚措施

上海网信办依据《中华人民共和国数据安全法》对该公司责令改正，给予警告，并处以人民币**五万元罚款**的行政处罚。

02

「2023年」



案例6：长沙某电商平台用户隐私数据存在泄露风险，未制定数据安全管理制度被处罚

案例 长沙某电商平台用户隐私数据存在泄露风险，未制定数据安全管理制度被处罚

案由

2023年2月，湖南省长沙市公安局岳麓分局网安部门工作发现，辖区某电商平台存在数据泄露隐患，迅速组织专业技术人员调取日志并约谈单位相关责任人员。经查，该企业服务器存在未授权访问漏洞，用户隐私数据存在泄露风险。通过进一步核实，该企业未制定数据安全管理制度、未充分落实网络安全等级保护制度。

处罚措施

长沙市公安局岳麓分局根据《中华人民共和国数据安全法》第27条、第45条第一款之规定，给予该企业**警告，并处罚款五万元，对直接责任人处罚款一万元，责令限期改正。**



案例7：湘潭某商旅服务公司票务系统，未采取技术措施保障数据安全被处罚

案例 湘潭某商旅服务公司票务系统，未采取技术措施保障数据安全被处罚

合规社
DATA COMPLIANCE

2023年2月，湖南省湘潭市公安局岳塘分局网安部门通过工作发现辖区某商旅服务公司票务系统中存有大量用户姓名、电话、身份证号、航班、银行账户等敏感数据，存在数据泄露风险。

案由

经查，该公司服务器短时间内存在大量登录失败，被恶意用户暴力破解账户密码痕迹。同时，服务器内安装的ElasticSearch软件，可通过互联网在无需账号密码条件下直接访问系统内敏感数据。

处罚措施 湘潭市公安局岳塘分局根据《中华人民共和国数据安全法》第27条、第45条第1款，给予该企业**警告，并责令限期改正**。



案例8：温州某科技公司将敏感数据上传至公有云，造成严重的数据泄露被处罚

案例 温州某科技公司将敏感数据上传至公有云，造成严重的数据泄露被处罚

案由

2023年3月，浙江某科技有限公司为浙江某县级市政府部门开发运维信息管理系统过程中，在未经建设单位同意的情况下，将建设单位采集的敏感业务数据擅自上传至租用的公有云服务器上，且未采取安全保护措施，造成了严重的数据泄露。

处罚措施

浙江温州公安机关根据《中华人民共和国数据安全法》第45条，对公司及项目主管人员、直接责任人员分别作出**罚款100万元、8万元、6万元**的行政处罚。



案例9：永州某物业人脸识别系统、车辆管理系统未履行数据安全保护义务被处罚

案例 永州某物业人脸识别系统、车辆管理系统未履行数据安全保护义务被处罚

2023年3月，湖南省永州市东安县公安局网安部门在查办一起侵犯公民个人信息案件中发现某小区业主信息泄露线索，随即对小区所属物业公司发起“一案双查”。

案由

经查，该公司使用的人脸识别系统、车辆管理系统中明文存有6000余名业主姓名、电话、身份证号、银行账户等敏感数据信息。

同时，人脸识别系统、车辆管理系统均存在登录账号弱口令，账号未设置权限管理，存放用户数据的办公电脑使用向日葵远程控制软件进行操作，且未采取任何安全防护措施，未履行数据安全保护义务。

处罚措施

永州东安县公安局根据《中华人民共和国数据安全法》第27条、第45条第1款，给予该公司**警告，并责令限期改正**。



案例10：江西某职业技术大学不履行数据安全保护义务被处罚

案例

江西某职业技术大学不履行数据安全保护义务被处罚

2023年3月，南昌市公安局工作发现，江西某职业技术大学师生个人信息疑似遭泄露。

案由

经查，该学校未健全全流程数据安全管理制度，未采取数据加密等相应技术措施保障数据安全，导致学校数据库被黑客非法入侵，师生个人敏感信息数据遭泄露。

处罚 措施

南昌市公安局依据《中华人民共和国数据安全法》第二十七条、第四十五条之规定，对该学校给予行政处罚。



案例11：怀化某燃气公司缴费系统账号密码为弱口令，未制定数据安全管理制度被处罚

案例 怀化某燃气公司缴费系统账号密码为弱口令，未制定数据安全管理制度被处罚

2023年3月，湖南省怀化市沅陵县公安局网安部门通过工作发现辖区某燃气公司缴费系统存有大量客户姓名、电话、身份证号、家庭住址等敏感数据。

案由

经查，该公司办公电脑未设置开机密码，缴费系统账号密码均为弱口令，并且该企业未制定数据安全管理制度、未充分落实网络安全等级保护制度。

处罚措施 怀化沅陵县公安局根据《中华人民共和国数据安全法》第27条、第45条第1款，给予该企业**警告，并责令限期改正**。



案例12：株洲某软件学校网站存在数据泄露风险，未履行数据安全保护义务被处罚

案例 株洲某软件学校网站存在数据泄露风险，未履行数据安全保护义务被处罚

案由

2023年3月，株洲市公安局荷塘分局网安大队接株洲市网络与信息安全信息通报中心通报，株洲某软件学校网站存在短文件名泄露漏洞。经网安大队检查发现，该网站系统中存在大量学生姓名、身份证号、电话号码、家庭住址等敏感信息。

该学校未对前述数据采取应有的技术保护措施，未履行数据安全保护义务，存在数据泄露风险。

处罚措施

株洲市公安局荷塘分局根据《中华人民共和国数据安全法》第45条第一款，给予该学校**警告，并责令限期改正**。



案例13：株洲某医院网站被篡改植入暗链，未履行数据安全保护义务被处罚

案例 株洲某医院网站被篡改植入暗链，未履行数据安全保护义务被处罚

案由

2023年3月11日，株洲市公安局荷塘分局网安大队接株洲市网络与信息安全信息通报中心通报，株洲某医院网站被篡改植入暗链，经网安大队检查发现，该医院管理平台日志系统中存储客户敏感数据，包括姓名、性别、身份证号、用药情况等敏感信息，该医院未对前述数据采取应有的技术保护措施，未履行数据安全保护义务，存在数据泄露风险。

处罚措施

株洲市公安局荷塘分局根据《中华人民共和国数据安全法》第四十五条第一款之规定，给予该医院**警告**，并责令限期改正。



案例14：邵东某医院没有开展正规数据安全教育培训，没有对个人信息去标识化被处罚

案例 邵东某医院没有开展正规数据安全教育培训，没有对个人信息去标识化被处罚

案由

2023年3月13日，邵东市公安局网络安全保卫大队民警对辖区单位开展网络安全和数据安全检查，在检查中发现某二类专科医院和某疫苗接种门诊没有制定数据安全管理制度和操作规程，没有对单位员工开展正规的数据安全教育培训，没有采取任何防篡改、防泄漏、防侵入等技术措施，没有对采集到的居民个人信息采取去标识化和加密措施，系统存在弱口令密码等严重数据安全隐患，均违反了《中华人民共和国数据安全法》第27条之规定。

处罚措施

邵东市公安局依据第45条规定，对上述两家单位予以行政**警告**处罚。



案例15：全南某公司未落实数据安全保护责任，未开展等级保护备案工作被处罚

案例 全南某公司未落实数据安全保护责任，未开展等级保护备案工作被处罚

案由

2023年4月，全南县公安局网安大队在开展网络和数据安全监督检查时，发现某公司疑似存在网络数据泄露隐患。随即，全南网警组织人员调取相关信息并约谈涉案人员。经查，该公司相关服务器存在未授权访问漏洞，用户隐私数据存在泄露风险。同时，未落实数据安全保护责任，未开展等级保护备案工作，相关数据安全保护规章制度形同虚设。该公司严重违反了《中华人民共和国数据安全法》第二十七条、第二十九条规定。

处罚措施

2023年4月21日,全南县公安局根据《中华人民共和国数据安全法》第二十七条、第四十五条之规定，给予该公司行政**警告**处罚，并责令限期整改。



案例16：洛阳某平台数据库未关闭免登录访问漏洞，造成平台数据泄露被处罚

案例 洛阳某平台数据库未关闭免登录访问漏洞，造成平台数据泄露被处罚

2023年4月3日，洛阳市新安县公安局网安部门接上级下发线索：新安县经济技术开发区某平台数据库疑似发生数据泄漏事件。

案由

新安县公安局网安部门立即对该公司进行了相关检查，调查发现该平台上线运行后未关闭免登录访问漏洞，存在重大网络安全隐患，导致平台数据泄漏。

处罚措施

新安县警方依据《网络安全法》第59条第一款，对新安县某区处以行政警告并责令整改；依据《中华人民共和国数据安全法》第27、45条，对该公司处以行政警告并处罚款**20万元**的处罚，并责令其对存在问题进行**整改**。



案例17：绥宁某催收公司非法获取债务人的信息，获取信息后也没有存档被处罚

案例 绥宁某催收公司非法获取债务人的信息，获取信息后也没有存档被处罚

案由

2023年4月4日，绥宁县公安局在工作中发现：XX乡XX村XX快递二楼成立一家催收公司，名称为XX达通仁信息技术咨询有限公司，法人代表张X，该公司在没有要求提供合法资质的情况下，审核交易双方的身份，在催收的过程中通过天眼查、小蓝本、钉钉等软件非法获取债务人的信息，获取信息后也没有存档。

处罚措施

违反《中华人民共和国数据安全法》第三十三条、第四十七条之规定，对XX达通仁信息技术咨询有限公司和其**法人代表张X予以行政处罚。**



案例18：湘潭某公司未落实数据安全管理制度，未开展数据安全教育培训被处罚

案例 湘潭某公司未落实数据安全管理制度，未开展数据安全教育培训被处罚

合规社
DATA COMPLIANCE

案由

2023年4月10日，第八个全民国家安全教育日来临之际，湘潭县公安局网安大队在开展网络、数据安全检查中，发现辖区某单位自建的应用系统中存储有该单位人员、财务信息等大量重要数据，但该单位未落实数据安全管理制度，未开展数据安全教育培训，且未对系统采取相应的技术防范措施，致使系统接口存在任意文件上传漏洞等数据安全隐患，大量个人信息、单位信息存在泄露风险。

处罚措施

根据《中华人民共和国数据安全法》相关规定，县公安局依法对该单位予以行政**警告**处罚，要求其切实履行主体责任，及时清理处置数据安全隐患。



案例19：江西某公司OA系统存储大量敏感数据，数据安全保护义务不到位被处罚

案例

江西某公司OA系统存储大量敏感数据，数据安全保护义务不到位被处罚

案由

2023年4月13日，接上级网信部门通报，江西某股份有限公司运营的网络智能办公系统疑似遭黑客组织攻击并植入木马病毒，主机存在受控的风险。当日，南昌市互联网信息办公室决定立案调查并派执法人员开展案件调查工作。经过现场勘验、抽样取证、远程勘验（样本技术分析）、笔录问询等程序，查明：①该公司的OA系统和服务器内存储了大量敏感数据，但该公司履行数据安全保护义务不到位，OA系统感染了可获取服务器文件管理权限和命令执行权限的木马程序，相关行为违反了《中华人民共和国数据安全法》第二十七条规定；②该公司开展数据处理活动未加强风险监测，在发现数据安全漏洞风险和事件时未采取补救措施，未履行风险监测、补救处置等义务，相关行为违反了《中华人民共和国数据安全法》第二十九条规定。

处罚措施

2023年5月30日，南昌市网信办依据《中华人民共和国数据安全法》第四十五条的规定，对江西某股份有限公司处以**警告、罚款50万元**，对直接负责的主管人员处以**罚款5万元**的行政处罚。



案例20：株洲某医院医疗管理系统存在数据泄露风险，未履行数据安全保护义务被处罚

案例 株洲某医院医疗管理系统存在数据泄露风险，未履行数据安全保护义务被处罚

案由

2023年4月20日，株洲市茶陵县公安局网安大队在进行日常网络安全检查工作中发现，茶陵县某医院的医疗管理系统存储着大量患者的姓名、身份证号、电话号码、家庭住址等敏感信息，该医院未建立数据安全管理制度，未采取任何的安全防护措施，未履行数据安全保护义务，存在数据泄露风险。

处罚措施

茶陵县公安局根据《中华人民共和国数据安全法》第27条、第45条第一款之规定，给予该医院**警告，并责令限期改正。**



案例21：石嘴山某通讯店未建立数据安全管理制度，违法办理手机卡被处罚

案例

石嘴山某通讯店未建立数据安全管理制度，违法办理手机卡被处罚

案由

2023年4月，石嘴山市大武口区分局网安大队、隆湖派出所案件办理中发现，犯罪嫌疑人刘某某等三人在大武口区隆湖某通讯店内，先后办理了14张手机卡，全部提供给境外犯罪分子用于电信网络诈骗。

分局网安大队快速反应，严查刘某某等三人异常的办卡行为。经询问，该通讯店在未询问办卡原由的情况下，就给刘某某等三人办理了14张手机卡用于违法犯罪活动。

依据公安部“一案双查”的要求，网安大队对该通讯店进行突击检查，发现其存在办公电脑未设置开机密码、未设置建立数据安全管理制度和未组织数据安全教育培训等违法行为。

处罚措施

分局网安大队依据《中华人民共和国数据安全法》第27条、第45条第1款，对该通讯店以未落实数据安全保护责任移交隆湖派出所进行处理，对其予以行政**警告处罚，责令限期整改。**



案例22-23：邵东市连开两张违反《中华人民共和国数据安全法》罚单

案例

邵东市连开两张违反《中华人民共和国数据安全法》罚单

2023年4月，邵东市网信办联合邵东市公安局等涉网管理部门积极开展联动执法，依照《中华人民共和国数据安全法》《湖南省网络安全和信息化条例》对两家单位负责人进行约谈，对两家单位予以行政警告处罚。

案由

邵东市网信办和市公安局网络安全保卫大队民警对辖区单位开展网络安全和数据安全检查时，发现辖区内两家单位疑似存在数据泄露风险。经查，两家单位没有制定数据安全管理制度和操作规程，没有对单位员工开展正规的数据安全教育培训，没有采取任何防篡改、防泄漏、防侵入等技术措施，用户个人信息数据存在泄露风险。

处罚措施

根据《中华人民共和国数据安全法》第四十五条和《湖南省网络安全和信息化条例》第二十六条、三十三条、第五十五条之规定，邵东市网信办联合市公安局对未履行数据安全保护义务的这两家单位负责人进行约谈，对两家单位依法予以行政警告处罚，要求切实履行主体责任，及时清理处置网络安全隐患。两家单位负责人均表示接受处罚并且立即按要求整改到位。



案例24：麻阳一商贸公司未履行数据安全保护义务被处罚

案例

麻阳一商贸公司未履行数据安全保护义务被处罚

合规社
DATA COMPLIANCE

案由

2023年4月，麻阳苗族自治县公安局网安大队在日常网络安全监督检查中发现某商贸公司未建立健全全流程数据安全管理制度，为组织开展数据安全培训，且该公司服务器内存有大量客户敏感数据，包括姓名、身份证号码、手机号码等信息，该公司未对敏感数据采取相应的技术保护措施，未履行数据安全保护义务。

处罚措施

根据《中华人民共和国数据安全法》的有关规定，麻阳公安对该公司未履行数据安全保护义务的违法行为，依法予以行政处罚。



案例25：怀化某手机店敏感信息资料数据文档未单独加密，存在泄露风险被处罚

案例 怀化某手机店敏感信息资料数据文档未单独加密，存在泄露风险被处罚

案由

2023年5月，怀化市溆浦县公安局西湖派出所民警在对溆浦县某手机店、某移动专营店等被处罚单位进行网络安全检查时发现，该店自2023年1月以来，将新开卡客户姓名、身份证号、手机号码等敏感信息资料数据文档，储存在店内未设置开机屏保密码的互联网电脑桌面上，且对该敏感信息资料数据文档未采取单独加设密码等相应的技术保护措施，存在泄漏风险。

处罚措施

根据《中华人民共和国数据安全法》第27条第1款、第45条第1款，对溆浦县某手机店予以行政处罚。



案例26：隆回某置业公司未履行数据安全保护义务被处罚

案例

隆回某置业公司未履行数据安全保护义务被处罚



案由

2023年5月，隆回县公安局网络安全保卫大队在查办一起侵犯公民个人信息案件中，发现某小区业主信息泄露线索，随即于2023年5月上旬联合隆回县局三阁司派出所对该小区的开发商邵阳市某置业公司发起“一案双查”。

经查，邵阳市某置业公司数据安全意识淡薄，未建立健全全流程数据安全管理制度，未开展数据安全教育培训，未采取相应的技术措施和其它必要措施保障公司的数据安全，导致该公司开发楼盘的所有业主信息被本公司工作人员多次贩卖。同时，该公司未明确数据安全负责人和管理机构，对存放置业业主用户数据的办公电脑未采取任何安全防护措施，未履行数据安全保护义务。

处罚措施

隆回县公安局根据《中华人民共和国数据安全法》第二十七条、第四十五条第一款之规定，给予该公司**警告**，并责令限期改正。



案例27：安庆某房地产公司未履行数据安全保护义务被处罚

案例

安庆某房地产公司未履行数据安全保护义务被处罚

案由

2023年5月，安庆市太湖县公安局网安大队、经济开发区派出所民警在对太湖县某房地产公司进行数据安全检查过程中，发现该公司数据安全意识淡薄，未建立数据安全管理制度和操作规程，未对员工开展数据安全教育培训，未对采集到的居民个人信息采取加密措施。

同时，该公司未明确数据安全负责人和管理机构，对存放业主用户数据的办公电脑未采取任何安全防护措施，未采取必要技术措施保障公司数据安全，未履行数据安全保护义务，导致大量数据信息面临泄露的重大风险。

处罚措施

太湖县公安局对该公司未履行数据安全保护义务的违法行为，依法处以**警告**并对直接责任人员处**罚款人民币1万元**的行政处罚。



案例28：昌平某软件公司未履行数据安全保护义务被处罚

案例

昌平某软件公司未履行数据安全保护义务被处罚



案由

2023年6月7日，昌平网安部门工作中发现，辖区内某软件有限公司研发的“某数据分析系统”存在数据泄露隐患。经查，该公司研发的“数据分析系统”内存有用户姓名、基因数据等数据信息。通过进一步核实，该系统内数据信息未采用加密措施，系统服务器未采取任何网络防护和技术防护措施，造成19.1GB公民隐私数据暴露在互联网。

处罚措施

北京市公安局昌平分局根据《中华人民共和国数据安全法》第二十七条、第四十五条第一款之规定，给予该企业**警告，并处罚款五万元人民币**，责令限期改正。



案例29：北京某科技公司APP后台存储的46万余条数据暴露在互联网上被处罚

案例 北京某科技公司APP后台存储的46万余条数据暴露在互联网上被处罚

案由

2023年6月13日，北京朝阳网安部门接市公安局网安总队通报，辖区某科技公司存在数据泄露隐患，分局迅速组织相关力量前往该科技公司进行现场网络安全检查。经工作发现，该科技公司一款APP产品后台存储的客户姓名、手机号、微信账号、邮箱等信息46万余条数据被暴露在互联网上，该数据一旦被不法分子获取，将导致大量公民个人信息泄露，给广大人民群众个人合法权益造成重大影响。

合规社
DATA COMPLIANCE

处罚措施

北京市公安局朝阳分局根据《中华人民共和国数据安全法》第二十七条、第四十五条第一款之规定，给予该科技公司**警告**的行政处罚。



案例30：衡阳某医院未履行数据安全保护义务被处罚，第三方技术公司也受处罚

案例 衡阳某医院未履行数据安全保护义务被处罚，第三方技术公司也受处罚

2023年6月，衡阳网信部门在数据安全领域开出的首张“罚单”。

案由

衡南县某医院未履行数据安全保护义务，造成部分数据泄露，违反《中华人民共和国数据安全法》第29条规定。



衡南县网信办依据第45条，对该医院作出责令整改、罚款5万元的行政处罚。同时，对第三方技术公司及相关责任人处以1.2万元罚款。

处罚措施

衡南县网信办依据《中华人民共和国数据安全法》第45条，对该医院作出**责令整改、罚款5万元**的行政处罚。同时，**对第三方技术公司及相关责任人处以1.2万元罚款**。



案例31：中山某科技公司对敏感数据未加密，未建立数据安全管理制度被处罚

案例 中山某科技公司对敏感数据未加密，未建立数据安全管理制度被处罚

2023年7月，中山市三乡公安分局鹤湾派出所对辖区内的公司进行数据安全检查过程中，发现一家信息科技公司疑似存在网络数据泄露隐患。

案由

通过询问相关责任人、调取网络设备日志信息、开展技术检测等方式，鹤湾派出所发现该公司在没有依法建立数据安全管理制度和操作规程等数据保护措施的前提下，对存储的公民敏感信息数据未采取去标识化和加密保护。

处罚措施

依据《中华人民共和国数据安全法》第27条、第45条，三乡公安分局对该公司处以**警告以及罚款5万元**的行政处罚，对**该公司负责人作出罚款1万元**的行政处罚。



案例32：重庆某科技公司未组织开展数据安全培训，被履行数据安全保护义务被处罚

案例 重庆某科技公司未组织开展数据安全培训，被履行数据安全保护义务被处罚

案由

2023年7月，根据有关部门移交的线索，重庆市网信办对属地一科技公司涉网络数据安全违法行为进行立案调查。经查，该公司因业务开展，收集、存储、处理的网络数据量较大，但未按法律法规要求建立健全全流程网络数据安全管理制度，未组织开展网络数据安全教育培训，未采取相应的技术措施和其他必要措施，保障网络数据安全等数据安全保护义务，且存在数据库数据泄露的情形。

处罚措施

重庆市网信办依据《中华人民共和国数据安全法》第二十七条、第二十九条、第四十五条之规定，对该公司作出责令限期改正，给予行政**警告**，**并处10万元罚款**的行政处罚。



案例33：南昌某高校发生数据泄露！罚款80万元，抓获3人！

案例

南昌某高校发生数据泄露！罚款80万元，抓获3人！

案由

2023年8月，南昌公安网安部门工作发现，南昌某高校3万余条师生个人信息数据在境外互联网上被公开售卖。

南昌公安网安部门立即开展一案双查，成功抓获犯罪嫌疑人3名。同时，对涉案高校不履行数据安全保护义务违法行为开展执法检查。

经查，涉案高校在开展数据处理活动中，未建立全流程数据安全管理制度，未采取技术措施保障数据安全，未履行数据安全保护义务，导致学校存储教职工信息、学生信息、缴费信息等3000余万条信息的数据库被黑客非法入侵，其中3万余条教职工、学生个人敏感信息数据被非法兜售。



处罚措施

南昌公安网安部门根据《中华人民共和国数据安全法》第四十五条的规定，对该学校作出责令**改正、警告并处80万元人民币罚款**的处罚，对主要责任人作出人民币**5万元罚款**的处罚。



案例34：因未制定数据安全管理制度，江苏淮安一足浴店被责令整改！

案例

因未制定数据安全管理制度，江苏淮安一足浴店被责令整改！

2023年8月，江苏公安执法公示平台公开了一份由江苏省淮安市公安局淮阴分局西坝派出所开具的行政处罚决定书，一家足浴店因未采取必要数据安全保障措施等被责令整改、警告。

案由

决定书显示，8月16日，西坝派出所的两位民警依法对一家名为六指情魔的足浴会所进行检查，发现该场所的电脑存储有顾客姓名、手机号码、身份证号码等敏感数据且未设置密码，未制定数据安全管理制度，未采取必要措施保障数据安全。

处罚 措施

西坝派出所根据我国《中华人民共和国数据安全法》相关规定，决定对该足浴会所处**以责令整改、警告**的行政处罚。



案例35：淮安蛋糕店因未组织数据安全培训及未建立数据安全管理制度等被处罚

案例

淮安蛋糕店因未组织数据安全培训及未建立数据安全管理制度等被处罚

案由

2023年8月10日，淮安市公安局淮安分局白马湖派出所民警对淮安区麦香人家蛋糕店履行数据安全保护义务情况进行检查。经查，该店因正常业务需要，开展会员数据处理活动，收集包含姓名、手机号等信息数据，但没有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。

该店作为数据处理者，未采取措施确保数据处理活动符合法律、行政法规的规定，并防止未经授权的访问以及数据泄露、篡改、丢失，属于未履行数据安全保护义务。

处罚措施

淮安区麦香人家蛋糕店的行为已构成未履行数据安全保护义务。根据《中华人民共和国数据安全法》第二十七条第一款、第四十五条第一款之规定，现决定对淮安区麦香人家蛋糕店**警告**。



案例36：南通某科技公司使用“弱口令”登录平台、未履行数据安全保护义务被处罚

案例 南通某科技公司使用“弱口令”登录平台、未履行数据安全保护义务被处罚

合规社
DATA COMPLIANCE

案由

2023年9月，江苏南通公安网安部门对当地某科技有限公司检查时发现，该公司对包含生产工艺流程、操作手册、员工个人信息等数据的MySQL数据库（数据量达百万条），未建立数据安全管理制度，也未采取相应技术措施保障数据安全，并且存在使用“弱口令”即可登录平台、访问数据的情况，涉嫌未履行数据安全保护义务。

处罚措施

南通公安机关依据《中华人民共和国数据安全法》第45条规定，对该公司予以行政**警告并责令限期改正**。



案例37：盐城某医药公司不履行数据安全保护义务被处罚

案例

盐城某医药公司不履行数据安全保护义务被处罚

案由

2023年9月，江苏盐城公安网安部门在对当地某医药公司检查时发现，该公司医疗健康信息的会员管理系统存有大量公民个人信息，经现场检测发现该系统存在网络安全漏洞，且该公司未建立数据安全管理制度，未组织开展数据安全教育培训，也未采取相应技术措施保障数据安全，涉嫌未履行数据安全保护义务。

处罚措施

盐城公安机关依据《中华人民共和国数据安全法》第45条规定，对该公司予以行政**警告并责令限期改正**。



案例

六盘水市某公司未履行数据安全保护义务被处罚

案由

2023年9月，贵州省六盘水市钟山区网安大队在办理一起帮助信息网络犯罪案时，犯罪嫌疑人供述其曾在六盘水钟山辖区某酒店客房内为境外诈骗份子搭建GOIP实施诈骗。钟山区网安大队立即对该酒店管理公司开展“一案双查”，对该公司在网络安全、数据安全方面存在的问题隐患进行排查，发现该公司使用的信息系统违规收集了酒店入住人员个人信息2万余条，系统存在安全隐患，数据泄露风险程度高。经六盘水网安支队对该信息系统的运维公司进行检查，发现该公司存在未履行数据安全保护义务、未建立数据安全管理制度和操作规程、未组织开展数据安全教育培训以及违规收集公民个人信息等违法行为。

处罚措施

综上，六盘水网安部门根据《中华人民共和国数据安全法》第四十五条（不履行数据安全保护义务的法律职责）第一款之规定，对该系统运维公司处以行政**警告并处行政罚款十万元**的处罚。



案例39：宿迁某医学检验机构不履行数据安全保护义务被处罚

案例

宿迁某医学检验机构不履行数据安全保护义务被处罚

合规社
DATA COMPLIANCE

案由

2023年9月，江苏宿迁公安网安部门对当地某医学检验机构检查时发现，该机构运营的医学检验信息平台存在SQL注入漏洞、弱口令等网络安全隐患，且未建立数据安全管理制度，未组织数据安全教育培训，未采取相应技术措施保障数据安全，未对其数据处理活动开展风险监测和定期风险评估，可致敏感业务数据泄露，涉嫌未履行数据安全保护义务。

处罚措施

宿迁公安机关依据《中华人民共和国数据安全法》第45条规定，对该机构予以行政警告并处罚款10万元。



案例40：成都某科技有限公司不履行数据安全保护义务被处罚

案例

成都某科技有限公司不履行数据安全保护义务被处罚

合规社
DATA COMPLIANCE

案由

2023年9月，江苏苏州公安网安部门工作发现，成都某科技有限公司在为苏州某信息科技股份有限公司相关系统运维过程中，未建立健全全流程数据安全管理制度，为图工作方便，私自将该公司30余万条运营数据上传至互联网，且未落实任何技术防护措施保障数据安全，未对其数据处理活动开展风险监测，可致该批数据泄露，涉嫌未履行数据安全保护义务。

处罚措施

苏州公安机关依据《中华人民共和国数据安全法》第45条规定，对该公司予以行政警告并处罚款5万元。



案例41：贵州某医院未制定数据安全管理制度、未履行数据安全保护义务被处罚

案例 贵州某医院未制定数据安全管理制度、未履行数据安全保护义务被处罚

案由

2023年9月，贵州省兴义市公安局网安大队在开展网络安全执法检查监督工作中，发现某医院信息系统存在反序列化漏洞。经查，该院信息系统存储个人身份信息50万条，攻击者可以轻易通过反序列化漏洞获取主机权限，并进入内网数据库中获取50万患者姓名、身份证号、亲属姓名电话等个人信息。

该院部分网络安全防护技术措施不到位，未制定数据安全管理制度、未履行数据安全保护义务。

处罚措施

兴义市公安局根据《中华人民共和国数据安全法》第四十五条第一款之规定，给予该医院**警告**处罚，并责令限期整改。



案例42：泰州某不动产登记中心和北京某科技发展研究中心不履行数据安全保护义务案

案例 泰州某不动产登记中心和北京某科技发展研究中心不履行数据安全保护义务案

合规社
DATA COMPLIANCE

案由

2023年9月，江苏泰州公安网安部门工作发现，当地某不动产登记中心的“业务练兵系统”存在Elasticsearch未授权访问安全漏洞，且未建立健全全流程数据安全管理制度，未落实有效的数据安全防护措施，可致该系统中存储的24万余条业务数据泄露，涉嫌未履行数据安全保护义务。

处罚措施

泰州公安机关依据《中华人民共和国数据安全法》第45条规定，对该不动产登记中心予以行政**警告并责令改正**；对该系统的建设运维单位北京某科技发展研究中心予以行政**警告并处罚款5万元**。



案例43：杭州某科技公司未履行数据安全保护义务被处罚

案例

杭州某科技公司未履行数据安全保护义务被处罚

2023年10月，根据国家网信办移交的问题线索，浙江省网信办依法对杭州某科技公司未履行数据安全保护义务的问题进行立案调查。

案由

经查实，该公司旗下某生活类APP相关数据库服务端口直接暴露在互联网环境中，存在未授权访问漏洞，未按要求履行数据安全保护义务，违反《中华人民共和国数据安全法》第二十七条之规定。

处罚 措施

浙江省网信办依据《中华人民共和国数据安全法》《行政处罚法》等法律法规，对杭州某科技公司作出**罚款5万元**的行政处罚，对该公司直接负责人作出**罚款1万元**的行政处罚。



案例44：存在数据漏洞风险，南昌市网信办依法对属地某企业作出行政处罚

案例 存在数据漏洞风险，南昌市网信办依法对属地某企业作出行政处罚

2023年10月，接上级网信部门通报，南昌县某企业存在数据漏洞风险，疑似出现删库勒索事件。经过立案调查、远程勘验、现场勘验、笔录问询等工作，查明：

案由

- 1.该企业运营的mongodb数据库存在未授权访问安全漏洞；
- 2.该企业未采取相应的技术措施和其他必要措施保障数据安全，其运营的数据库被黑客删库并勒索；
- 3.该企业未加强风险监测，发生删库勒索事件时未采取处置措施和履行主动报告义务。该企业的相关行为违反了《中华人民共和国数据安全法》第二十七条、二十九条的规定。

处罚措施

南昌市网信办依据《中华人民共和国数据安全法》第四十五条的规定，对该企业作出**警告并处罚款5万元**、对直接负责的主管人员作出**罚款1万元**的行政处罚。



案例45：保靖某幼儿园无数据安全管理制度，存在严重的个人信息数据泄露风险被处罚

案例 保靖某幼儿园无数据安全管理制度，存在严重的个人信息数据泄露风险被处罚

案由

2023年10月17日，保靖县公安局网安大队在进行网络数据安全检查时，发现保靖县某幼儿园存储在电脑中存有700余条学生及家长个人信息的文档未采取技术加密保护措施，无数据安全管理制度，存在严重的个人信息数据泄露的风险隐患。

处罚措施

该幼儿园违反了《中华人民共和国数据安全法》的相关规定，保靖县公安局对该幼儿园给予行政**警告**处罚，并责令整改。



案例46-48：北京市网信办对三家企业未履行数据安全保护义务作出行政处罚

案例

北京市网信办对三家企业未履行数据安全保护义务作出行政处罚

2023年11月，根据国家网信办移交的问题线索，北京市网信办依据《中华人民共和国数据安全法》对属地三家企业涉嫌存在网络数据安全违法行为进行立案调查并作出行政处罚。

案由

经查实，三家企业违反《中华人民共和国数据安全法》第二十七条规定，未履行数据安全保护义务，部署的ElasticSearch数据库存在未授权访问漏洞，造成部分数据泄露。

处罚措施

北京市网信办依据《中华人民共和国数据安全法》第四十五条第一款规定，对三家企业分别作出责令改正，给予**警告，并处5万元罚款**的行政处罚，对直接主管人员和其他责任人员处以**1万元罚款**处罚。



案例49：邵阳某科技公司不履行数据安全保护义务被处罚

案例

邵阳某科技公司不履行数据安全保护义务被处罚

2023年11月，邵阳县公安局网安大队组织精干力量对全县企业进行了网络安全执法检查，检查过程中依法查处了1家不履行网络安全保护义务的公司，有效预防了网络安全事件的发生，净化了全区网络空间。

案由

11月16日，网安大队在检查中发现，湖南某科技有限公司负责承建开发邵阳县高新技术产业开发区，未按照法律法规建立网络安全等级保护制度，未履行数据安全保护义务，存在网络安全隐患，给网络安全秩序造成不良影响。

处罚 措施

根据《中华人民共和国数据安全法》相关规定，目前，湖南某科技有限公司被公安机关**责令改正并予以行政警告**处罚。



案例50：温州某大药房因未履行数据保护义务被处罚110万元

案例

温州某大药房因未履行数据保护义务被处罚110万元

2023年11月，温州网安部门在日常工作中发现有人在暗网上售卖温州某大药房销售数据。通过侦查发现，该大药房数据分析师利用工作便利将大量交易数据导出并售卖。

案由

温州网安在依法对该数据分析师采取刑事强制措施的同时，启动“一案双查”工作机制。经进一步侦查发现，该大药房因未建立健全全流程数据安全管理制度，未组织开展数据安全教育培训，未采取相应的技术措施和其他必要措施保障数据安全，最终导致大量敏感数据泄露。

处罚措施

该大药房数据分析师因违反《中华人民共和国刑法》第二百五十三条之一之规定，涉嫌侵犯公民个人信息罪被温州公安机关依法刑事拘留，现案件还在进一步办理中。同时，温州公安机关依据《中华人民共和国数据安全法》第二十七条、第四十五条之规定，对该公司处**罚款110万元**，对该大药房直接负责的主管人员处**罚款10万元**。



案例51：上海市某科技公司因数据泄漏被依法处罚

案例

上海市某科技公司因数据泄漏被依法处罚

2023年12月，工作中发现，上海市某科技公司相关数据库存在未授权访问漏洞，部分数据被窃并传输到境外。上海市网信办将相关情况通报涉事企业并要求立即核查整改，但该科技公司无视数据安全保护责任，未进行及时有效整改且擅自将涉事数据库一删了之，意图逃避处罚。上海市网信办依据《中华人民共和国数据安全法》对该科技公司及公司直接责任人员予以行政处罚。

案由

经调查核实，该科技公司主要从事为保险类企业提供互联网通信服务。2022年10月，公司安装配置了一台Elasticsearch数据库服务器，用于搜集多个应用系统的业务日志，并存储了包含用户姓名、身份证号码、手机号在内的大量个人信息。该公司未建立健全全流程数据安全管理制度，未采取相应的技术措施和其他必要措施保障数据安全，因数据库存在未授权访问漏洞，造成部分数据泄漏被传输到境外IP。同时企业私自删除涉事数据库逃避责任、没有按照规定及时向网信部门报告，未有效履行数据安全保护义务。

处罚措施

针对以上违法情况，上海市网信办依据《中华人民共和国数据安全法》第二十七条、第四十五条，对该科技公司作出**责令改正，给予警告，并处人民币8万元罚款**的行政处罚；对公司直接责任人员作出**罚款人民币1万元**的行政处罚。



案例52：珠晖某医院未履行数据安全保护义务，被依法追究法律责任！

案例 珠晖某医院未履行数据安全保护义务，被依法追究法律责任！

2023年12月，珠晖公安分局网安大队加大对相关单位的检查力度，并给予一家医院行政警告处罚。

案由

12月15日，民警对辖区某医院网络安全管理、数据安全保护、网络应急预案检查时，发现该医院的档案系统使用弱口令，且长时间没有更换密码，导致敏感信息面临较大泄露风险，无法有效保障数据安全。

处罚措施

根据调查结果，珠晖公安分局依据《中华人民共和国数据安全法》第二十七条和第四十五条第一款之规定，给予该医院行政警告处罚。



案例53：赣州某公司网络营销代理业务中未保障数据安全被处罚

案例

赣州某公司网络营销代理业务中未保障数据安全被处罚

合规社
DATA COMPLIANCE

近日，根据上级部门通报，江西赣州某信息技术公司业务系统疑似遭受黑客攻击，存在数据泄露风险。

案由

江西省通信管理局立即依法组织开展案件调查，查明该公司在开展网络营销代理业务中未有效落实网络和数据安全保护主体责任，未依法采取相应的技术措施保障业务系统数据安全。

处罚 措施

该行为违反了《中华人民共和国数据安全法》相关规定，省通信管理局对赣州某信息技术公司给予**警告、罚款15万元**，对直接负责的主管人员和直接责任人各**罚款1万元**。

03

「2024年」





案例54：重庆某科技公司未建立完善的络数据安全管理制度被罚款10万元

案例

重庆某科技公司未建立完善的络数据安全管理制度被罚款10万元

2024年3月，重庆市网信办发现某一科技公司存在网络数据安全违法行为，并进行立案调查。重庆网信办依据《中华人民共和国数据安全法》作出责令限期改正，给予行政警告，并处10万元罚款的行政处罚。

案由

调查结果显示，该公司运营的某OA信息系统由于未履行网络数据安全保护义务，导致大量数据泄露，情节严重。作为网络数据处理者，该公司未按法律规定建立完善的全流程网络数据安全管理制度，也未组织开展网络数据安全教育培训，同时未采取必要的技术和其他措施确保网络数据安全。这些行为违反了《中华人民共和国网络安全法》、《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》等相关法规。

处罚措施

依据《中华人民共和国数据安全法》第二十七条、第二十九条、第四十五条之规定，重庆网信办对该公司作出责令限期改正，给予行政警告，**并处10万元罚款**的行政处罚。



案例55：南昌某集团未履行数据安全保护义务，向境外传输大量数据被处罚

案例

南昌某集团未履行数据安全保护义务，向境外传输大量数据被处罚

2024年5月，接上级网信部门通报，南昌某集团有限公司所属IP疑似被黑客远程控制，频繁与境外通联，向境外传输大量数据。经过立案调查、现场勘验、远程勘验（采样技术分析）、笔录问询等工作，查明：



案由

- 1.该公司未履行数据安全保护义务，未采取相应的技术措施和其他必要措施保障数据安全，所属的服务器遭境外黑客攻击并植入可获取服务器文件管理权限和命令执行权限的木马程序，大量数据疑似泄露或被窃取，相关行为违反了《中华人民共和国数据安全法》第二十七条规定；
- 2.该公司开展数据处理活动未加强风险监测，在发现数据安全漏洞风险和事件时未采取补救措施，未履行风险监测、补救处置等义务，相关行为违反了《中华人民共和国数据安全法》第二十九条规定。

处罚措施

南昌市网信办依据《中华人民共和国数据安全法》第四十五条的规定，对该公司处以**警告、罚款10万元**，对直接负责的主管人员处以**罚款2万元**的行政处罚。



案例56：长沙某公司未履行网络数据安全义务被行政处罚

案例

长沙某公司未履行网络数据安全义务被行政处罚

案由

2024年6月，湖南长沙某企业网络信息系统数据安全保护、应急处置、风险评估等制度不健全，存在高危风险。



处罚措施

长沙市委网信办依据《中华人民共和国数据安全法》对该企业及相关责任人分别作出**罚款5万元和1万元**的行政处罚，**并责令整改**。



案例57：衡阳某公司因未履行网络数据安全义务被行政处罚

案例

衡阳某公司因未履行网络数据安全义务被行政处罚

衡阳市网信办经核查发现，某科技公司在衡阳从事软件业务开发工作，因开发应用的网站数据库存在未授权访问漏洞，泄露了公民的个人信息。

案由

该公司在开展数据处理活动时未建立健全全流程数据安全管理制度，未组织开展数据安全教育培训，未采取相应的技术措施和其他必要措施保障数据安全，造成公民个人信息泄露。

处罚措施

依据《中华人民共和国数据安全法》第四十五条，衡阳市网信办对该科技公司作出**责令改正，予以警告，并处10万元的行政处罚。**



案例58-63：甘肃甘州公安查处6起酒店行业未履行数据安全保护义务案

案例

甘肃甘州公安查处6起酒店行业未履行数据安全保护义务案

案由

近日，甘州分局网安大队在工作中发现，张掖市某酒店管理服务有限公司等6家酒店，网络数据管理系统均存在数据泄漏的风险，未履行好数据安全保护义务，严重影响公民个人信息安全。



处罚措施

根据《中华人民共和国数据安全法》相关规定，对6家酒店依法给予行政处罚，责令立即整改。



《中华人民共和国数据安全法》第27条

开展数据处理活动应当依照法律、法规的规定，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。

《中华人民共和国数据安全法》第29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；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

《中华人民共和国数据安全法》第33条

从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。

《中华人民共和国数据安全法》第35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。

《中华人民共和国数据安全法》第45条

开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。