

关键词：陕西信息保护

内容概要：

陕西省关于加强信息保护的若干规定第一章 总则第一条 为加强我省信息保护与管理，规范信息处理行为，保障信息安全，维护国家安全和社会公共利益，保护公民、法人和其它组织的合法权益，根据有关法律、法规和规章，结合我省实际，制定本规定。第二条 本省内...

正文：

陕西省关于加强信息保护的若干规定

第一章 总则

第一条 为加强我省信息保护与管理，规范信息处理行为，保障信息安全，维护国家安全和社会公共利益，保护公民、法人和其它组织的合法权益，根据有关法律、法规和规章，结合我省实际，制定本规定。

第二条 本省内数据处理过程中的信息收集、转移、存储、恢复、加工、使用、删除、销毁等活动适用本规定。法律、法规另有规定的，从其规定。本规定所称信息是指为特定主体所持有的，适合于通过网络与信息系统或其它电子媒介制作、存储、加工、处理、发送、传输、接收的数据、图像、声音等。

本规定所称的个人信息是指上述信息中能够识别公民个人身份和涉及公民个人隐私的信息。

第三条 本省数据处理过程中的信息保护，应遵循合法、公正、必要的原则。

合法原则是指信息处理应遵守我国现有的法律法规的规定，不得侵害它人合法权益，不得损害国家利益和社会公共利益；

公正原则是指信息处理必须征得相关政府机关、企业或个人的许可或同意；

必要原则是指收集的信息的数量应在达到处理目的条件下最小化，不得收集与信息使用目的无关的信息。

第二章 部门职责

第四条 下列部门按照各自职责做好信息保护的相关工作：

(一) 工信部门负责信息保护的综合协调、指导、监督工作。依法制定信息保护管理制度。组织制定相关行业的从业规范及标准。对从业人员开展安全教育和培训。协调处置与信息保护相关的投诉与质询。

(二) 各部门、各机构、各单位负责本部门、本行业、本机构、本单位内的信息保护工作。

(三) 公安、安全、保密和机要等部门负责对信息收集、处理和使用过程中出现的非法信息买卖、转移、泄露等违法犯罪活动进行打击和查处。

(四) 工商部门在企业年度报告时，应将从事数据恢复行业的法人、其它组织遵守行业的从业标准和规范情况列为报告事项。

第三章 信息处理

第五条 信息收集必须具有明确、合法的目的，信息的收集方法与范围必须合法、正当。

第六条 收集地理、人口、统计等国家基础信息和企事业单位的重要商业信息或敏感信息，应当依法履行相关手续。

第七条 收集个人信息，应当符合下列要求：

(一) 个人明确同意；

(二) 与个人存在合同关系或类似关系，为完成合同义务必须进行个人信息收集；

(三) 为保护个人的重要利益、第三人的合法权益或社会公共利益；

第八条 收集个人信息应明确将个人信息收集者的身份与住所、个人信息的使用目的、使用范围、留存期限及个人信息文件的公开方式与地点等重要事项告知该个人。个人信息收集者应该确保所收集的个人信息完整正确，并规定“个人”对于本人信息具有确认、修订和停止利用的权利。

第九条 未经主管部门审批，法人、其它组织及个人不得向第三方转移收集国家基础信息；未经法人、其它组织及个人同意，不得向第三方转移个人信息及企业重要商业信息或敏感信息。

第十条 在转移信息前，应当评估信息接收者是否具有信息安全保障能力，并应当通过合同方式明确信息接收者的信息保护责任，避免信息受到未经授权的访问、篡改、泄露、删除、毁损。

第十一条 禁止向境外转移国家基础信息。境外包括位于境外的个人或境外注册的组织和机构。

第十二条 对存有国家基础信息资源、企业重要商业信息或敏感信息、个人信息的计算机信息系统和存储介质要确保安全。对重要信息应当进行备份，备份介质必须保存在安全环境中，非常重要的信息应异地存储。

第十三条 未经主管部门审批，法人、其它组织及个人不得擅自加工和使用国家基础信息；未经法人、其它组织及个人同意，不得擅自加工和使用个人信息、企业重要商业信息或敏感信息。

第十四条 不得超出信息收集时所披露的使用目的和范围加工或使用信息。

第十五条加工和使用信息时，应当采取下列措施，确保信息安全：

- (一) 避免任何对信息未经授权的访问；
- (二) 避免任何对信息未经授权的披露、复制、修改、删除；
- (三) 核实处理操作的合法性。

第十六条发生或者可能发生信息泄露、毁损、丢失时，应立即采取补救措施，防止损失扩大；造成或者可能造成严重后果的，应在24小时之内向主管部门报告，主管部门作出处理决定前，可要求相关组织或个人暂停信息收集和处理工作。

第十七条未经主管部门审批，法人、其它组织及个人不得超过留存期限或无法实现信息处理目的时擅自留存国家基础信息；未经法人、其它组织及个人同意，不得超过留存期限或无法实现信息处理目的时擅自留存个人信息、企业重要商业信息或敏感信息。执法机构调查取证时，应采取适当的存储和屏蔽措施。

第十八条收集、转移、存储、恢复、加工、使用、删除、销毁涉密信息时，应严格按照保密法规定执行。

第四章 数据恢复服务管理

第十九条 从事数据恢复业务的单位和个人应当严格遵守上述信息安全规定，禁止未经授权处理信息，对进行恢复的信息应当采取必要的技术和管理措施，防止未经授权的访问、传播、披露、更改和删除。

第二十条从事数据恢复业务的法人、其它组织和个人，应当符合相关的从业标准和规范的要求。

第二十一条数据恢复行业的从业人员应当符合相关从业标准和规范的要求，并与从业机构签订聘用合同及保密协议，承担保密义务。

第二十二条对保存在台式机硬盘、笔记本硬盘、服务器硬盘、存储磁带库、移动硬盘、U盘、数码存储卡、MP3等存贮介质上丢失的数据进行恢复时应遵守如下规定：

- (一) 数据恢复前应对信息持有者的有效身份证明存档，并确认信息持有者合法持有恢复数据；

应得到信息持有者的明确同意，并与其签订保密协议；

恢复法人或其他组织的数据，须经该法人或其他组织负责人同意。

- (二) 数据恢复过程中，应建立专人负责制，保证设备专机专用，未经信息所有者授权不得使用、处理、泄露客户数据，信息持有者有权全程监督；

- (三) 数据恢复完毕后，信息持有者有权自己验证数据、监督数据拷贝，数据恢复单位或个人应及时销毁恢复数据，并提供手段供数据所有者查证存储介质无其它备份；

- (四) 数据恢复业务不得转包。

第五章 监督与检查

第二十三条 任何组织或个人发现非法收集、转移、存储、恢复、加工、使用、删除国家基础信息资源、企业重要商业信息或敏感信息、个人信息时，可向工信部门或行业协会进行举报或者投诉。

第二十四条工信部门或行业协会接到举报或者投诉后，应及时协调相关部门对举报或者投诉内容进行核实，督促其依法作出处理或者移送有权部门处理。

第二十五条工信部门可综合协调各行政管理部门检查从事数据处理过程中的信息安全防范工作，协调开展相关检查活动，处置突发事件和重大问题。

第二十六条实施监督检查时，可以要求从事数据处理的机构和人员提供相关材料，进入其生产经营场所调查情况，从事数据处理的机构和人员应当予以配合。

第二十七条违反本《规定》的行为，依照相关法律法规予以处罚。构成犯罪的，依法追究刑事责任。侵害他人民事权益的，依法承担民事责任。

第六章 附则

第二十八条 本规定不适用于国家机关为保障国家安全、打击犯罪、执行公务而进行的数据处理；不适用于公民在纯粹的个人或家庭活动中所进行的数据处理；不适用于法人或其它组织所处理的数据数量较少，不会对国家安全、公共利益或个体权利造成侵害的数据处理。

第二十九条本规定自2014年4月1日起施行，至2017年4月1日起废止。

西安弈聪信息技术有限公司简介

西安弈聪立足陕西西安，为西安企业提供网站优化，软件开发，软件外包，电子政务，网站建设、企业网络营销咨询服务及实施为主体业务，为客户提供一体化IT技术服务。

西安弈聪现有技术架构包含PHP,asp,.NET.C++,VB,J2EE等，在MYSQL,MSSQL数据库系统，ORACLE大型数据库管理系统开发方面专长，经验丰富，是业内技术服务最全面，技术实力最雄厚的IT技术服务企业之一。

