RELIABLE NETWORK
SAFE WORLD
TOPSEC

《个人信息保护法》全文逐条解读

天融信
TOPSEC

北京市海淀区西北旺东路 10 号院西区 11 号楼东侧天融信科技集团

邮编：100193

电话：+8610-82776666

传真：+8610-82776677

服务热线：+86-4007770777

http://www.topsec.com.cn

原文	**解读**
第一章总则	
第一条 为了保护个人信息权益,规范个人信息处理活动,促进个人信息合理利用,根据宪法，制定本法。	本条明确了《个人信息保护法》的立法目的。其核心是通过规范个人信息处理活动，在保障信息权利人法定权益的基础上，促进对个人信息的合理利用。立法依据是我国宪法，体现了《个人信息保护法》重视维护公民人格尊严和人格自主的深层含义。
第二条 自然人的个人信息受法律保护,任何组织、个人不得侵害自然人的个人信息权益。	本条明确了自然人依法享有个人信息权益，相较于《民法典》等其他法律，《个人信息保护法》首次提出自然人享有“个人信息权益”。
第三条 组织、个人在中华人民共和国境内处理自然人个人信息的活动,适用本法。 在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动,有下列情形之一的,也适用本法:(一)以向境内自然人提供产品或者服务为目的;(二)分析、	《个人信息保护法》采取了地域范围+公民和/或居民相结合的适用范围，赋予了必要的域外适用效力，能够更好地维护我国境内自然人的个人信息权益。并明确了 2 个相应情形：1.向境内自然人提供产品或者服务；2.分析、评估境内自然人的行为；对于在中国境外处理

评估境内自然人的行为;(三)法律、行政法规规定的其他情形。	中国境内自然人个人信息，在下文中有具体要求。
第四条 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。 个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。	本法中个人信息是指：“以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。”在此之前诸多的立法中已对其有了定义，如《网络安全法》规定，“个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。”《民法典》规定：“个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电话号码、电子邮箱、健康信息、行踪等。”

	可以看出本法中“个人信息”的定义面更广，将个人信息的范围从此前的“可识别性“扩大到“可识别性+可关联性”，同时去除了列举式的表述方式，删除了《网络安全法》对个人信息限定于“个人身份”相关的范围，定义更趋向范化，保护范围更广。
第五条 处理个人信息应当采用合法、正当、必要和诚信原则,不得通过误导、欺诈、胁迫等方式处理个人信息。	在《网络安全法》、《民法典》中均有要求个人信息需遵从采用合法、正当的方式，不得通过欺诈、误导等方式处理个人信息。在二审稿中新增了对于“胁迫”方式的法律限制，包含了弱势一方违背了自主意愿选择同意的场景，意图是更好的保护弱势一方的自主权。
第六条 第六条处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。	与《网络安全法》、《民法典》中要求一致，在处理个人信息时，应根据目的实现“最小必要原则”

收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。	
第七条 处理个人信息应当遵循公开、透明的原则,公开个人信息处理规则,明示处理的目的、方式和范围。	需要告知个人个人信息的处理方式及目的，确保在公开、透明的环境下开展个人信息处理活动
第八条 处理个人信息应当保证个人信息的质量,避免因个人信息不准确、不完整对个人权益造成不利影响。	个人信息处理结果的错误，除可能影响到个人信息处理者提供的产品或者服务的质量以外，也可能会对个人权益带来负面影响，故有必要保证个人信息的质量，确保个人信息的准确性以及完整性。
第九条 个人信息处理者应当对其个人信息处理活动负责,并采取必要措施保障所处理的个人信息的安全。	明确个人信息处理者对个人信息的处理活动要承担安全保障义务，有责任采取相应的措施避免个人信息泄露、篡改等安全风险的发生。
第十条 任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。	危害国家安全、公共利益是任何行为活动都不可触及的底线，处理个人信息活动一样，除了不能损害个人权益外，国家安全、公共利益同样不得被侵害。本条将个人信息的处理活动提升至国家安全、公共利益的高度，对此，个人信

	息处理者在个人信息的处理活动中，不仅要遵守本法的规范，还要关注其他特定领域的限制性规定，例如生物基因信息等与国家安全相关的信息处理活动。
第十一条 国家建立健全个人信息保护制度,预防和惩治侵害个人信息权益的行为,加强个人信息保护宣传教育,推动形成政府、企业、相关行业组织、社会公众共同参与个人信息保护的良好环境。	国家将会健全个人信息相关的保护制度，同时个人信息保护也需我们全社会共同参与，包括政府、企业、各行业到我们公民。
第十二条 国家积极参与个人信息保护国际规则的制定,促进个人信息保护方面的国际交流与合作,推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等的互认。	我们也将参与个人信息保护国际规制的制定，说明我国在促进产业发展的同时需要加强个人信息保护领域的立法、规范和标准制定，不仅要展现产业的硬实力，还要展现“中国标准”的制度软实力。
第二章个人信息处理规则	
一般规定	

第十三条 符合下列情形之一的,个人信息处理者方可处理个人信息:(一)取得个人的同意;(二)为订立或者履行个人作为一方当事人的合同所必需;(三)为履行法定职责或者法定义务所必需或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需;(四)为应对突发公共卫生事件,或者紧急情况下为保护自然人的生命健康和财产安全所必需;(五)依照本法规定在合理的范围内处理已公开的个人信息;(六)依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息;(七)法律、行政法规规定的其他情形。依照本法其他有关规定,处理个人信息应当取得个人同意,但有前款第二项至第七项规定情形的,不需取得个人同意。	《网络安全法》中规定了需征得“被收集者同意”这样的唯一的处理个人信息合法性条件，《民法典》中规定在满足“知情同意、已公开、维护公共利益的情形，行为人不承担民事责任”，但均未进行进一步解释。在《个人信息保护法》中给出了七种需满足之一的情形方可处理个人信息，充分考虑了在实际实践的各种场景。具体为：一、取得个人同意；二、为履行合同所必需，一方面签订合同在某种意义上为知情同意的一种形式，另一方面也要求了所有的处理活动的目的应将履行合同为唯一目的，也具体包含了劳务场景中签订集体合同的实际场景;三、为履行法定职责或者法定义务所必需，在此情形下需在其他法律法规规定的充足基础上，方可进行处理，为各行业行使监管等职责的处理行为提供依据；四、为应对突发公共卫生事件,或者紧急情况下为保护自然人的生命健康和财产安全所必需;在此情形下，与公共利益及涉及到生命财

	产安全的紧急避险相比、法律对个人权益影响的考量将进行适当的考量和让位，此处体现了个人信息的公共属性，在具体执行过程中，要关注必需”这一特定边界；五、依照《个人信息保护法》规定在合理的范围内处理已公开的个人信息，此情形在《民法典》中也有相关描述，若是自然人自行公开，意味着在某种意义上同意他人对这些个人信息进行处理，但此情形下是需要谨慎考量合理范围的边界和标准；六、为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息，此情形下可以联想到在疫情期间，对确诊患者疫情期间的流调公示信息，通常都对个人信息匿名化了，且仅公布了疫情防控所需的行程等信息，体现了“合理使用”的原则；七、法律、行政法规规定的其他情形，此处为将来可能存在的情形留有空间。“

第十四条 处理个人信息的同意,应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的,从其规定。个人信息的处理目的、处理方式和处理的个人信息种类发生变更的,应当重新取得个人同意。	个人主体只有在充分知晓处理活动的信息后才能更好的作出对自身权益影响的判断，对此，法律保护公民个人的充分知情权，包括“个人信息处理的目的、方式、种类等”，以上事项需由个单独或者书面同意，且当这些因素产生变化时也应及时告知个人，且再次取得同意。
第十五条 基于个人同意而进行的个人信息处理活动,个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。个人撤回同意,不影响撤回前基于个人同意已进行的个人信息处理活动的效力。	法律赋予了个人对已经同意的个人信息处理活动享有撤回权，本法第十三条无需取得个人同意的情况除外。在个人提出撤回时，处理者应提供便捷的方式，如在提供显著、简便的退订渠道、客服等服务。个人信息的撤回同意不具备溯及力，不影响撤回前基于个人同意而产生的个人信息处理活动及其结果，有效减轻了处理者在响应个人信息主体权利时的顾虑和成本。
第十六条 个人信息处理者不得以个人不同意处理其个人信息或者撤回其对个人信息处理的同意为由,拒绝提供产品或者服务;处理个人信息属于提供产品或者服	个人主体提出撤回要求，并不意味着在授权期间的数据处理是无效的，存储的数据、加工的数据仍然可以使用或若个人信息属于提供的产品或者服务所必

务所必需的除外。	需的则除外。
第十七条 个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项（一）个人信息处理者的名称或者姓名和联系方式；（二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；（三）个人行使本法规定权利的方式和程序；（四）法律、行政法规规定应当告知的其他事项。前款规定事项发生变更的，应当将变更部分告知个人。个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。	此处在实践场景中更多的是体现在隐私条款中，除要求告知个人信息处理相关的具体事项外，也要求告知的方式是可以易于查阅和保存的，在个人信息采集前，通过显著方式、清晰易懂的隐私条款（或其他形式）告知个人信息处理的目的、方式、处理的个人信息种类、联系方式等信息，并在其内容方式变化、新增信息处理者等情况时，再次取得个人同意。同时需关注当个人涉及到不满 14 岁未成年人时，应单独取得其父母或者受委托监护人的同意。并在不同情形及时的更新隐私条款。
第十八条 个人信息处理者处理个人信息,有法律、行政法规规定应当保密或者不需要告知的情形的,可以不向个人告知前条规定的事项。紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的,个人信息处理者应当在紧急情况	与第十三条中处理个人信息无需征得个人同意中的相应条款有关，但本条规定紧急情况下，虽然在事前、事中可以不取得当事人同意，但是在事后是需要“及时告知”。

消除后及时告知。	
第十九条 除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。	在一般情况下个人信息的保存应在数据处理目的所需要的最短时间，但是很多法律法规中对个人信息相关内容存储的明确期限，则也应符合达到合规要求。
第二十条 两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的,应当约定各自的权利和义务。但是,该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。个人信息处理者共同处理个人信息,侵害个人信息权益的,应当依法承担连带责任。	数据采集之后在实际场景中，时常会出现有两个甚至多个数据控制者，本法中明确若其中一方侵害到了个人权益，则另一方需承担连带责任，故在考虑引入第三方共同控制相应数据时，应做好充足的资质考虑等工作，具体也可参照，在《信息技术 个人信息安全规范》中第 9.6 条 共同控制者中有相应的条款。

第二十一条 个人信息处理者委托处理个人信息的,应当与受托方约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等,并对受托方的个人信息处理活动进行监督。受托方应当按照约定处理个人信息,不得超出约定的处理目的、处理方式等处理个人信息;委托合同不生效、无效、被撤销或者终止的,受托方应当将个人信息返还个人信息处理者或者予以删除,不得保留。未经个人信息处理者同意,受托方不得转委托他人处理个人信息。	此条的"委托方"与上一条中的"共同处理者"不同，委托方不具备个人信息的控制权，也不需要承担连带责任，受委托方更应通过合同等形式明确受委托方的责任，做好对委托方的监督，当合同不生效、被撤销或者终止时，应将个人信息及时收回，或者采取有效的手段监督其删除。
第二十二条 个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当向个人告知接收方的名称或者姓名和联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。	当出现合并、分立等情形时，需向个人信息权利人告知接收方的"身份、联系方式"，处理者不再需要取得个人的同意，但当变更处理目的和方式的时候，需要再次征得个人同意。

第二十三条 个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。	在实际的场景中可能会存在因提供产品或服务，需要将处理过的个人信息提供给第三方的情况，当出现这种情形时，处理者需要及时的告知个人，并取得个人的同意。当接收方的处理目的和方式发生变更后，数据处理者也需再次取得个人的同意。
第二十四条 个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。 通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。 通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。	目前给自动化决策作出界定，：“是指通过程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、监控、信用状况等，进行自动化决策的活动。要求个人信息处理者保证自动化决策的透明度和结果的公平、公正，不得通过自动化的决策使得个人权益受到损害，当对个人权益造成重大影响时，个人主体有权拒绝，平衡了信息处理者与个人主体不对等的矛盾。

第二十五条 个人信息处理者不得公开其处理的个人信息,取得个人单独同意的除外。	在处理个人信息活动中，公开个人信息可能会对个人主体权益带来影响，所以需要当公开个人信息时，需要取得个人同意，当然第十三条规定的情形除外。
第二十六条 在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。	明确了关于在场所进行图像拆解、个人身份识别，如人脸识别的相应要求，其原则都应是为了确保公共安全为唯一目的，与第十三条为实现公共利益相对应。若有其他用途时，需要单独取得个人的同意，在实际操作中可能会存在一定的难度，需要慎重考虑是否还进相应活动。
第二十七条 个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。	此条款可以与二十六条公开取得同意、二十七条在公共场所采集的图像信息及个人身份识别信息这类在某种程度公开的信息的要求及第十三条可以处理个人信息的情境进行一并理解。
第二节敏感个人信息的处理规则	

第二十八条 敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。 只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。	在《个人信息保护法》出台之前，《民法典》规定了隐私权和个人信息，并把一部分个人信息通过隐私权的方式进行保护，但是《民法典》没有关于个人敏感信息的规定。《个人信息保护法》中个人敏感信息破坏后对“尊严”的损害与《民法典》中隐私的定义“影响生活安宁和不愿意被他人知晓”有一定的重合。个人隐私更多的偏向主观个人主体感受为出发的判断，而敏感个人信息更偏向客观的标准界定。
第二十九条 基于个人同意处理敏感个人信息的,个人信息处理者应当取得个人的单独同意。法律、行政法规规定处理敏感个人信息应当取得书面同意的,从其规定。	敏感信息需要取得个人的单独同意。
第三十条 个人信息处理者处理敏感个人信息的，除本法第十七条第一款规定的事项外，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照本法规定可以不向个人告知的除外。	在处理敏感信息时，取得单独同意外，还需要告知个人对个人权益的影响影响程度

第三十一条 个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。	《儿童个人信息网络保护规定》第九条规定“网络运营者收集、使用、转移、披露儿童个人信息的，应当以显著、清晰的方式告知儿童监护人，并应当征得儿童监护人的同意”，《民法典》则要求，“任何组织或者个人不得披露未成年人的个人隐私”，这当然不是一般规定的范畴。《个人信息保护法》略微降低了要求，要求“取得父母或者其他监护人的同意“，但个人信息处理者在进行处理之前需采取一定的手段判别被处理人的年龄，从而避免违法此条规定。
第三十二条 法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的,从其规定。	这里给除了例外情况，为根据法律法规规定或者取得行政许可的除外。
第三节国家机关处理个人信息的特别规定	
第三十三条 国家机关处理个人信息的活动,适用本法;本节有特别规定的,适用本节规定。	国家机关处理处理个人信息时需满足本法规规定。

第三十四条 国家机关为履行法定职责处理个人信息,应当依照法律、行政法规规定的权限、程序进行,不得超出履行法定职责所必需的范围和限度。	国家机关在旅行处理个人信息时也应当在法律法规所规定的职责范围内，需有法可依。
第三十五条 国家机关为履行法定职责处理个人信息，应当依照本法规定履行告知义务；有本法第十八条第一款规定的情形，或者告知将妨碍国家机关履行法定职责的除外。	国家机关处理个人信息一般情况也需告知个人，取得统一，但是由于国家机关的特殊性，可能存在告知同意后影响执法效果的可能，故这种情况可不用告知，也于本法第十三条相呼应。
第三十六条 国家机关处理的个人信息应当在中华人民共和国境内存储;确需向境外提供的,应当进行风险评估。风险评估可以要求有关部门提供支持与协助。	明确要求国家机关处理的个人信息需要存储在中国境内，当向境外提供时，需要进行风险评估，对应到第三章 个人信息跨境提供的规则。
第三十七条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息,适用本法关于国家机关处理个人信息的规定。	本条与《数据安全法》第四十二条相似，明确了法律法规授权的管理公共事务的组织在处理个人信息需依照本章的规定，扩大了本章的适用范围。
第三章 个人信息跨境提供的规则	

第三十八条 个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；（二）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；（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；（四）法律、行政法规或者国家网信部门规定的其他条件。中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。	本法规定因业务需要确需向境外提供个人信息时，需满足以下条件之一：“通过网信部门组织的安全评估、经专业机构进行个人保护认证、签订网信部门制定的标准合同模板、或法律法规规定的其他条件。”
第三十九条 个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人	除满足上条要求外，还需取得个人的单独同意，并且告知境外方的联络方式，以便个人可以了解和及时维护对个人权益产生的影响。

的单独同意。	
第四十条 关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者,应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的,应当通过国家网信部门组织的安全评估;法律、行政法规和国家网信部门规定可以不进行安全评估的,从其规定。	这里重点对关键基础设施运营者和处理个人信息达到一定规模的处理者提出了严格的要求，因为当他们的个人信息一旦泄露，将可能会严重危害国家安全、经济安全、社会稳定、公众健康和安全的业务，后果十分严重。故当他们需像境外提供数据时，一般情况只适用于第三十八条 第一款，都需通过网信部门的安全评估方可对尽快提供。
第四十一条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者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个人信息。	与《数据安全法》三十五条保持一致，在数据安全法发布之前，可以实现域外管辖。

第四十二条 境外的组织、个人从事损害中华人民共和国公民的个人信息权益,或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的,国家网信部门可以将其列入限制或者禁止个人信息提供清单,予以公告,并采取限制或者禁止向其提供个人信息等措施。	在涉及跨境情形的时候，由网信部门采取限制或者禁止提供的清单的机制，可参照商务部颁发的《不可靠实体清单规定》中建立不可靠实体清单制度。
第四十三条 任何国家和地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的,中华人民共和国可以根据实际情况对该国家或者该地区对等采取措施。	与《数据安全法》第二十五条保持一直，体现了我国在对待歧视性的禁止、限制等措施的反制态度。
第四章个人在个人信息处理活动中的权利	
第四十四条 个人对其个人信息的处理享有知情权、决定权,有权限制或者拒绝他人对其个人信息进行处理;法律、行政法规另有规定的除外。	个人主体对个人信息具有自决权和知情权，需要在充分个人信息处理的具体情况和对自身的影响后，决定限制或进行个人信息的处理，但有法律法规规定的除外。

第四十五条 个人有权向个人信息处理者查阅、复制其个人信息；有本法第十八条第一款、第三十五条规定情形的除外。个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。	此处与《民法典》第一千零三十七条相对应，指自然对个人信息的查阅复制权，信息主体有权查阅其个人信息处理情况，并有权对处理的个人信息进行复制。同时也新增了“可携带”权，这里对个人信息处理者有了更高的要求。
第四十六条 个人发现其个人信息不准确或者不完整的,有权请求个人信息处理者更正、补充。个人请求更正、补充其个人信息的,个人信息处理者应当对其个人信息予以核实,并及时更正、补充。	此处与《民法典》第一千零三十七条相应对应，指自然对个人信息的更正权，信息主体有权请求信息处理主体对不正确、不全面的个人信息进行更改与补充的权利，既包括错误更正和补充权。
第四十七条 有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：（一）处理目的已实现、无法实现或者为实现处理目的不再必要；（二）个人信息处理者停止提供产品或者服务，或者保存期限已届满；（三）个人撤回同意；（四）个人信息处理者违反法律、行政法规或者违反约定处理个人信息；（五）法律、行	《网络安全法》第四十三条、《民法典》第一千零三十七条都规定了个人信息的删除权，本法在此基础上对删除权做了细化规定，一方面明确了信息处理者的主动删除义务，同时也细化了可删除的法定情形和例外情形，在实际操作层面，使得删除权更具有可执行性。具体表现为：在法定或者约定的事由出现时，处理者应当主动删除其处理的个人

政法规规定的其他情形。法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。	信息，自然人也具有要求个人信息处理者删除其个人信息的权利。同时本法也规定了未到法律法规规定的保存期限和删除个人信息从技术上难以实现的删除例外情况，在不能删除的情况下，个人信息处理者应当停止除了存储之外的处理活动并采取有效的安全措施。
第四十八条 个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。	此处与第四十四条知情权相呼应，在实际场景中可能会出现需要个人信息处理者对处理规则进行解读，已便个人信息主体充分知晓的情况。
第四十九条 自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。	与《民法典》第九百九十四条规定关于死者人格利益权的保护相对应，及死者的近亲可以行使关于死者的个人信息的权利，包括知情权、决定权、删除权、复制权等。同时，法律也赋予了死者在生前确定个人信息县官权利执行方式的决定权。
第五十条 个人信息处理者应当建立个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的,应当说明理由。	此处为保障个人在数据处理中的权利，要求个人信息处理者建立起受理个人行使权利的申请机制、一般体现为信息

	处理者应当建立畅通、有效的投诉举报渠道、客服服务渠道等。
第五章 个人信息处理者的义务	
第五十一条 个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失:(一)制定内部管理制度和操作规程;(二)对个人信息实行分类管理;(三)采取相应的加密、去标识化等安全技术措施;(四)合理确定个人信息处理的操作权限,并定期对从业人员进行安全教育和培训;(五)制定并组织实施个人信息安全事件应急预案;(六)法律、行政法规规定的其他措施。	从管理和技术多个方面要求了个人信息处理者对于个人信息的安全风险防范包括：1）制度建设上，通过制定管理制度明确负责个人信息安全的负责的组织、人员。制定适合于企业自身业务特点的管理要求，通过制定细化的操作规程，从而管控具体业务中对个人信息的处理目的、处理方式、个人信息的种类以及对个人的影响、可能存在的安全风险等。2）分类保护上，在《数据安全法》中要求对数据进行分类分级保护，而此处要求个人信息处理者的个人信息实行分类管理，作为企业来说，首先需要区分一般个人信息和敏感个人信息，通过以类定级，确定需采取的相应的保护措施。3）技术措施上，采集到个人信息后，应采用相应的加密、去标识化等技术手段，确保个人信息被未

	授权的访问，确保个人信息得到有效的管控。如当在前台页面展示个人信息时，采取脱敏的手段，在数据库存储个人信息时，采用加密的技术手段等。4）个人信息处理操作权限上， 通过良好的访问控制、账号权限管理、细颗粒的的权限设置做好个人信息处理人员操作权限管理，并通过定期的数据安全审计， 确保个人信息操作权限的合理配置，及有效管控。5）安全事件应急上，制定适合自身业务场景的个人信息安全事件应急预案， 并定期开展应急演练，提高个人信息安全事件的应急响应能力。6）同时保护法律法规规定的其他要求。
第五十二条 处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人,负责对个人信息处理活动以及采取的保护措施等进行监督。个人信息处理者应当公开个人信息保护负责人的联系方式,并将个人信息保护负责人的姓名、联系方式等报送履行个	当处理个人信息的梳理达到规定时，需定个人信息保护负责人,负责对个人信息处理活动以及采取的保护措施等进行监督。个人信息处理者应当公开个人信息保护负责人的联系方式,并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。具体

人信息保护职责的部门。	实施可以参照国家标准或者行业相关要求，也可参照《信息技术 个人信息安全规范》第 11 章具体执行。
五十三条 本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。	由境外机构于境内设立的专门机构或指定代表承担个人信息保护责任的规定曾见于《个人信息出境安全评估办法(征求意见稿)》第二十条，目的在于通过对境外个人信息处理者于境内设立的专门机构或指定代表的管辖而间接实现对境外个人信息处理者的管辖。
第五十四条 个人信息处理者应当定期对其个人信息处理活动遵守法律、行政法规的情况进行合规审计。	个人信息处理者需要在个人信息处理活动的过程中，定期的开展对个人信息合规的审计工作，确保活动长期处于安全、合规的状态
第五十五条 有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录：（一）处理敏感个人信息；（二）利用个人信息进行自动化决策；（三）委托处理个人信息、向其他个人信息处理者提供个人信	在进行高风险操作时应进行风险评估包括：处理敏感个人信息、利用个人信息进行自动化决策、进行自动化决策时、委托他人处理时、向境外提供时、在对个人权益有重大影响时。

息、公开个人信息；（四）向境外提供个人信息；（五）其他对个人权益有重大影响的个人信息处理活动。	
第五十六条 个人信息保护影响评估应当包括下列内容：（一）个人信息的处理目的、处理方式等是否合法、正当、必要；（二）对个人权益的影响及安全风险；（三）所采取的保护措施是否合法、有效并与风险程度相适应。个人信息保护影响评估报告和处理情况记录应当至少保存三年。	以及要求评估报告的保存期限最少是三年。可以使得数据处理者在关键业务活动中，及时的发现风险，规避风险。
第五十七条 发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：（一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；（二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；（三）个人信息处理者	规定要求了个人信息处理者在发现个人信息泄露之后的应对措施，包括需告知个人信息保护的职责部门和个人，同时也说明在未造成损害影响时，可以不用告知个人信息主体，但履行个人信息保护的职责部门，有权对泄露后对个人主体的损害程度进行判别，并可要求处理者通知个人。

的联系方式。 个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。	
第五十八条 提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务：（一）按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；（二）遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；（三）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；（四）定期发布个人信息保护社会责任报告，接受社会监督。	对规模巨大的互联网平台提出了增强要求，除了需确保自身个人信息保护的安全外还需监督平台内产品和服务提供者个人信息处理活动的合法合规，承担“守门人角色”。主要包括：一、建立个人信息保护合规制度体系，并由外部独立的机构对前进行监督，确保监督出现的问题可以在尽量少的障碍下得到反馈；二、制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；三、对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；四、需要定期发布个人信息保

	护社会责任报告，接受社会监督。
第五十九条 接受委托处理个人信息的受托人，应当依照本法和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务	对于需遵循的对象的范围都会有比较明确的要求，此条也同样是明确了受委托方也应遵循本章要求。
第六章履行个人信息保护职责的部门	
第六十条 国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。 国务院有关部门依照本法和有关法律、行政法规的规定,在各自职责范围内负责个人信息保护和监督管理工作。 县级以上地方人民政府有关部门的个人信息保护和监督管理职责,按照国家有关规定确定。 前两款规定的部门统称为履行个人信息	对履行个人信息保护的职能部门进行了明确，网信部门为数据安全管理的主管部门负责统筹协调，由国务院的有关部门在各自行业内负责监管，在纵向上到县级。

保护职责的部门。	
第六十一条 履行个人信息保护职责的部门履行下列个人信息保护职责:(一)开展个人信息保护宣传教育,指导、监督个人信息处理者开展个人信息保护工作;(二)接受、处理与个人信息保护有关的投诉、举报;(三)调查、处理违法个人信息处理活动;(四)法律、行政法规规定的其他职责。	规定了职责部门的具体的保护工作,包括宣传教育、举报投诉、调查监督等。
第六十二条 国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作:(一)制定个人信息保护具体规则、标准;(二)针对小型个人信息处理者、处理敏感个人信息以及人脸识别、人工智能等新技术、新应用,制定专门的个人信息保护规则、标准;(三)支持研究开发和推广应用安全、方便的电子身份认证技术,推进网络身份认证公共服务建设;(四)推进个人信息保护社会化服务体系	规定了国家网信部门和国务院有关部门除了履行个人信息保护职责的部门还应组织制定个人信息保护的相关规则和标准,推进个人信息保护社会化服务体系建设,并承担支持有关机构开展相关评估、认证服务的责任。其中重点提到了人脸识别、人工智能、方便的电子身份认证等。

建设，支持有关机构开展个人信息保护评估、认证服务；（五）完善个人信息保护投诉、举报工作机制。	
第六十三条 履行个人信息保护职责的部门履行个人信息保护职责,可以采取下列措施:(一)询问有关当事人,调查与个人信息处理活动有关的情况;(二)查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料;(三)实施现场检查,对涉嫌违法个人信息处理活动进行调查;(四)检查与个人信息处理活动有关的设备、物品;对有证据证明是违法个人信息处理活动的设备、物品,向本部门主要负责人书面报告并经批准,可以查封或者扣押。履行个人信息保护职责的部门依法履行职责,当事人应当予以协助、配合,不得拒绝、阻挠。	明确相关部门可以采取的措施，一方面为相关部门实施的履职行为提供法律依据，使其在履职时有法可依，另一方面也有助于其履职过程中的行政相对人了解相关部门的职责范围，实现对相关部门履职行为的有效监督。

第六十四条 履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施，进行整改，消除隐患。 履行个人信息保护职责的部门在履行职责中，发现违法处理个人信息涉嫌犯罪的，应当及时移送公安机关依法处理。	这里赋予了个人信息保护部门，在发现了较大风险和已发生个人信息安全事件后的约谈职能，同时也支持委托专业的机构对个人信息处理活动进行的合规审计。
第六十五条 任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理,并将处理结果告知投诉、举报人。 履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。	此处对第六十一条第二款进行了补充，并明确了任何组织和个人都有权提起举报和投诉，并将公布相关联系方式，为未来个人权益受到侵害后，个人需求保护职能部门的保护提供了支撑。
第七章 法律责任	

第六十六条 违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。	若个人信息处理者违法《个人信息保护法》规定，将会由省级以上履行个人信息保护职责的部门对企业和主管个人信息的个人进行处罚，情节严重的，没收违法所得，并处五千万元以下或者上一年度营业额百分之五罚款，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。相较于之前的所有的法律，可谓是最严的处罚，提高了企业的违规成本，起到了更强的警示作用。

第六十七条 有本法规定的违法行为的,依照有关法律、行政法规的规定记入信用档案,并予以公示。	在已颁布的《电子商务法》、《儿童个人信息网络保护规定》、《侵害消费者权益行为处罚办法》中都启用了信用档案的机制，在除影响营业、罚款以外增加了企业名誉这一类处罚，处罚力度进一步增大。
第六十八条 国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。 履行个人信息保护职责的部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。	对国家机关不履职有两种形式：一是被责令改正，二是负责人员被处分。需注意的是前一种方式责令的主体除了该国家机关的上级机关还包括履行个人信息保护职责的部门，这体现了对国家机关的追责既属于国家机关特有的对上级负责机制，又体现了归口专业监管的性质。
第六十九条 处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。 前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定;个人因此受到的损失和个人信息处理者因此获得的利益难以确定	与《民法典》第一千一百八十二条规定的侵害人身权益情形下的侵权相对应，明确了个人信息保护侵权责任的过错原则。

的，根据实际情况确定赔偿数额。	
第七十条 个人信息处理者违反本法规定处理个人信息,侵害众多个人的权益的,人民检察院、履行个人信息保护职责的部门和国家网信部门确定的组织可以依法向人民法院提起诉讼。	对于违反本法规定处理个人信息，侵害众多个人的个人信息权益的行为，可以提起公益诉讼。该等行为属于《民事诉讼法》规定的“损害社会公共利益的行为”，属于可以提起个人信息公益诉讼的情形。
第七十一条 违反本法规定,构成违反治安管理行为的,依法给予治安管理处罚;构成犯罪的,依法追究刑事责任。	将责任从一般违法、侵权责任上升为治安责任或刑事责任的规定，个保法为刑法提供了前置。
第八章 附则	
第七十二条 自然人因个人或者家庭事务处理个人信息的,不适用本法。法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的,适用其规定。	规定了本法的不适用范围。

第七十三条　本法下列用语的含义:(一)个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。(二)自动化决策,是指利用个人信息对个人的行为习惯、兴趣爱好或者经济、健康、信用状况等,通过计算机程序自动分析、评估并进行决策的活动。(三)去标识化,是指个人信息经过处理,使其在不借助额外信息的情况下无法识别特定自然人的过程。(四)匿名化,是指个人信息经过处理无法识别特定自然人且不能复原的过程。	对本法中的用语进行了明确的解释，包括个人信息处理者、自动化决策、去标识化和匿名化。
第七十四条　本法自2021年11月1日起施行。	本法将于2021年11月1日正式实施