RELIABLE NETWORK
SAFE WORLD
TOPSEC

《个人信息保护法》合规路径指引

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

1 出台背景

1.1 个人信息安全保护刻不容缓

随着网络信息技术和数字经济的快速发展，给公民生活带来便利的同时，个人信息安全事件频发，如：“知名招聘平台恶意**倒卖用户简历**、APP 过度索权**超范围收集个人信息、人脸识别滥用、大数据杀熟**”等，被侵犯的公民个人信息数量从‘倍数级’进阶至‘指数级’，呈现爆炸式增长。尤其当下正处在共同抗击新冠疫情的特别时期，几乎每位公民都被密集的采集了行踪信息、人脸识别信息，公众对后续可能产生的个人信息安全问题心存担忧，**亟需有这样一部专门的法律来保护公民的隐私和生命财产安全、回馈社会的关切。**

1.2 国外个人信息保护相关立法情况

从全球个人信息保护相关的立法来看，欧洲与美国最早关注到个人信息保护相关的问题，并逐步出台了个人信息保护相关的法律。1970 年，德国黑森州制定了首部《数据保护法》，1876 年联邦德国制定了《个人资料保护法》，包括了全面的个人信息保护规范。1980 年，由经合组织通过《隐私保护和个人信息跨境流动指南》明确了个人信息保护的“合法正当、知情同意、保证质量”等 8 大原则 2018 年，经过欧盟议会长达四年的讨论，欧盟出台了《通用数据保护条例》，这一保护条例被称为“史上最严数据保护条例”，至今已有多家公司因违法该条例面临了巨额的罚款。美国在个人信息保护方面并没有统一的立法，注重对个人信息的利用，所以无论是个人信息权的范围还是具体内容都较窄，规定主要以市场为导向，依靠行业自律，加州作为先行者在 2020 年通过了《加州消费者隐私权》。另外，各国在相关法律中都明确了域外管辖的范围和要求，如 GDPR 中要求只要对在欧盟境内的主体提供商品或服务都需遵守相关条款约束，**我国也需要有这样的一部法律，使得我国公民个人信息保护具有域外效应。**

1.3 我国个人信息保护相关立法情况

事实上我国已经有多部法律、法规以及规章涉及个人信息保护，比如《刑法》及其修正案、《民法典》、《消费者权益保护法》、《网络安全法》、《电子商务法》、《未成年人保护法》等等都作出了相关的规定，但是从整体看存在分散的立法状态，需要根据形势的发展，制定**有针对性的专门法律来加以规范，形成合力。**个人信息本身具有社会性和公共性，需要**让渡一部分权利以实现社会的公共利益和国家安全**，不应当仅因某些信息可识别或可联系某个人而赋予其对这些信息的绝对支配权，个人信息具备社会属性，需要有一部立法奠定个人保护的正当性基础。我国从实际出发，深入总结网络安全法等法律、法规、标准的实施经验，将行之有效的做法和措施上升为法律规范。

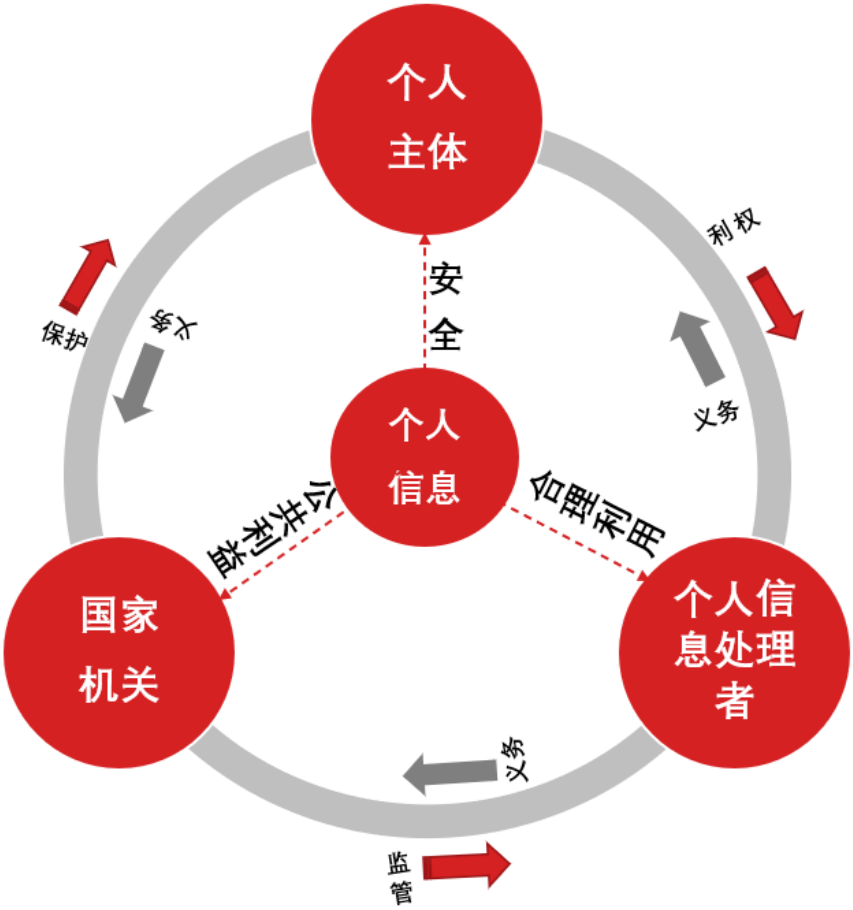
1.4 《个人信息保护法》结构

《个人信息保护法》三审稿于 2021 年 8 月 20 日在十三届全国人大常委会第三十次会议表决通过，将在 2021 年 11 月 1 日实施。《个人信息保护法》**作为我国的一项个人信息保护的基础法律**，明确了个人信息保护的原则，区分了一般个人信息和敏感个人信息的处理规则，以及涉及到跨境提供个人信息的相关规则；明确了个人信息主体在个人信息处理活动中的权利、个人信息处理者的义务、履行个人信息保护的监管职责及严格的法律责任。全文共 8 章 74 条。


中华人民共和国个人信息保护法
一、总则
1.目的
2.宗旨
3.范围
4.定义
5.合理、正当、必要
6.目的明确、最小化
7.公开、透明
8.保证质量
9.安全保护义务
10.不得非法处理
11.环境构建
12.积极开展国际交流与合作
二、个人信息处理规则
第一节 一般规定
13.可处理情形
14.知情同意
15.撤回同意
16.不得拒绝同意
17.告知要求
18.例外情况
19.存储期限
20.共同处理
21.委托处理
22.个人信息转移
23.向他人提供
24.自动化决策
25.公开个人信息
26.公共场所采集
27.处理已公开个人信息
第二节 敏感个人信息的通用规则
28.敏感个人信息定义
29.单独同意
30.必要性告知
31.未成年人信息
32.行政许可
第三节 国家机关处理个人信息的特别规定
33.适用性
34.范围和限度
35.告知义务
36.境内存储
37.公共事务管理组织
三、个人信息跨境提供的规则
38.可提供情形
39.单独同意
40.关键信息基础设施要求
41.外国司法或者执法机构
42.限制清单
43.对等反制
四、个人在个人信息处理活动中的权利
44.知情权、决定权
45.查阅权、复制权
46.更正、补充权
50.建立便捷的个人行使权利的申请受理和处理机制
47.删除权
48.有权要求解释说明
49.代行使死者权利
五、个人信息处理者的义务
51.基本保护义务
52.规定规模处理者义务
53.境外个人信息处理者
54.合规审计
55.个人影响评估
56.评估内容
57.安全事件处置
58.大型互联网平台义务
59.受托人义务
六、履行个人信息保护职责的部门
60.职责部门
61.保护职责
62.保护工作内容
63.履职措施
64.约谈审计机制
65.投诉举报机制
七、法律责任
66.行政处罚
67.信用档案
68.国家机关责任人的处罚
69.过错原则
70.公益诉讼
71.刑事责任
八、附则
72.不适用范围
73.术语解释
74.施行时间

2 三方平衡的哲学

2.1 个人权益与合理利用的平衡



为解决个人主体与个人信息处理者能力之间不对等的问题，《个人信息保护法》通过加强对个人主体的保护，明确了包括国家机关在内的个人信息处理者处理个人信息的合法性条件，以及管理责任部门的保护职责，力求在个人权利保护与个人信息合理利用上达到平衡，从而实现安全的个人信息、健康的市场生态、最大化的社会利益。

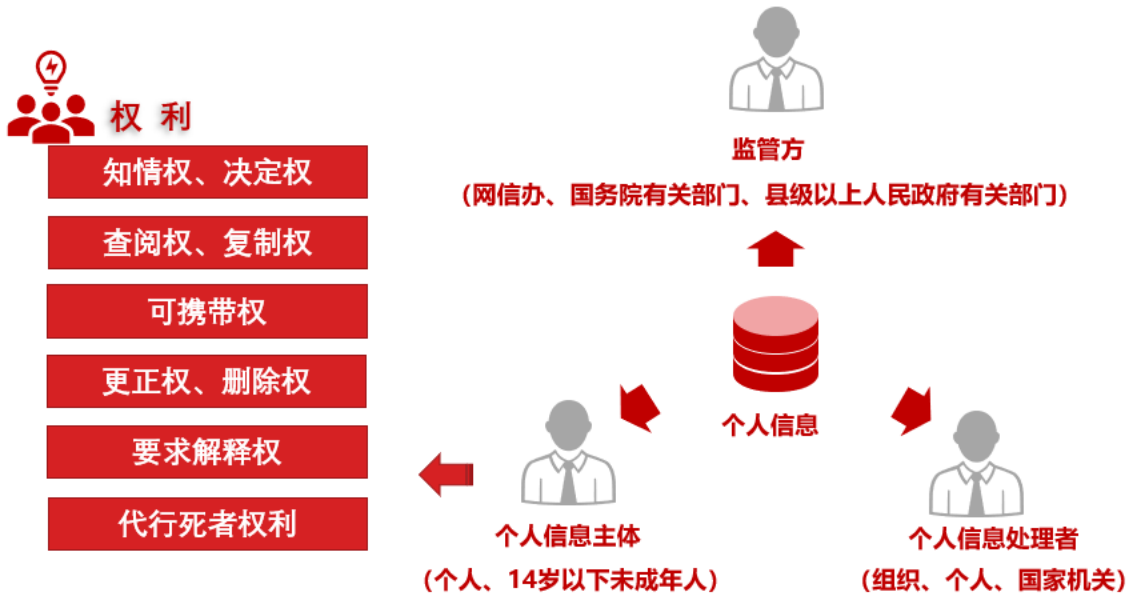
2.2 加强了对个人主体的保护

2.2.1 加大了被保护的范围

《个人信息保护法》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，如在《网络安全法中》“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。”在《民法典》中 “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《个人信息保护法》中“个人信息”的定义面更广，从此前的**“可识别性”**扩充为**“可识别性”+“可关联性”**，同时去除了列举形式，及删除了《网络安全法》中“个人身份”的限制性定语，使得定义更趋向范化，个人信息被保护的范围更广。

2.2.2 明确了个人信息主体的权利



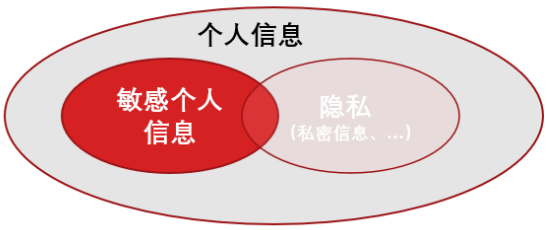
2.2.3 约束了大数据杀熟、公共场所采集行为

自动化决策在日常生活中可能会给个人权益带来重大影响，在大数据算法加持下甚至出现了很多以隐私为条件的“隐私驱动模式”产业，而作为个人信息主体很难与之抗衡，成为弱势一方。《个人信息保护法》对自动化决策的规则进行规范，要求透明化算法、提供不针对个人特征的选项、不得提供差别待遇，可以

有效的遏制大数据杀熟对个人主体的不公平待遇。

明确了关于在场所进行图像采集、个人身份识别，如人脸识别的相应要求，要求其采集动机都应是为了**确保公共安全为唯一目的，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，如**在采集到之后还需注意进一步履行安全保护义务**。

2.2.4 加强了对 “敏感个人信息”的保护



《个人信息保护法》：
- 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

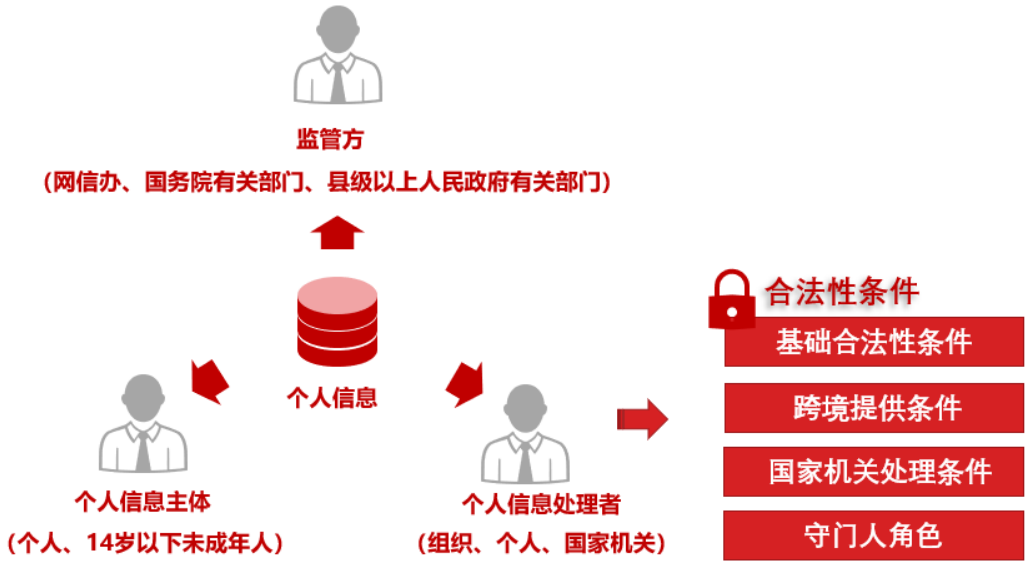
《民法典》
- 自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动和私密信息；

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。**

《个人信息保护法》给出了敏感个人信息的定义，**并着重强调了不满十四周岁未成年人的个人信息**。与在《信息安全技术　个人信息安全规范》中的定义有所区别在示例上也做了范围上的缩小，不包含身份证件号码等，**保证了在实践中可以更好的落地执行**。但也**提出了更为严格的要求**，处理敏感信息时除了**需单独的取得个人主体同意**，还需向个人告知处理敏感个人信息的必要性以及对个人的影响。相关法律、行政法规对处理敏感个人信息有规定的，还应当取得相关行政许可或者作出其他限制。

注：《个人信息保护法》中敏感个人信息包括种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等信息。”

2.3 明确了个人信息处理者处理个人信息合法性条件



2.3.1 基础合法性条件

《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，与公共利益相比、个人权益的影响的考量将不再放在首位，此处也体现了个人信息的公共属性；**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；**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。

2.3.2 明确跨境提供个人信息条件

《个人信息保护法》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”。这样多元监管路径，保障了企业跨境数据传输的便利，提高了跨境提供数据的效率。另外还需取得个人的单独同意，并且告知境外方的联络方式，以便个人有渠道及时维护对个人权益产生的影响。

对于关键信息基础设施运营者同时还需关注《关键基础设施安全保护条例》、中关于出境的相关要求。

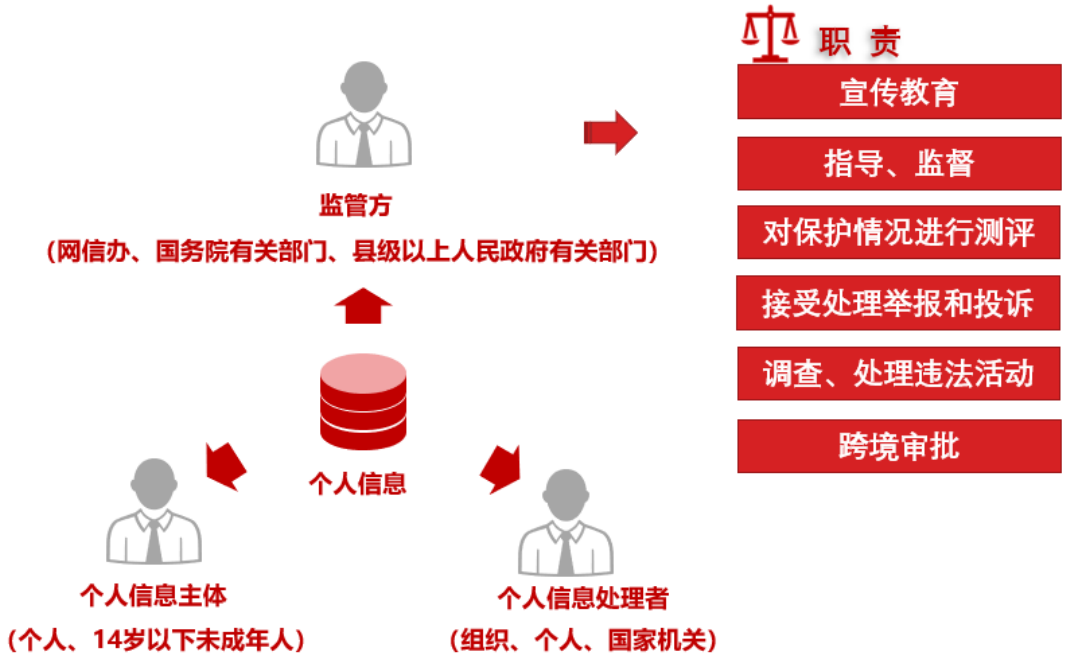
注：跨境安全评估相关内容可参考国家网信办于 2019 年 6 月 13 日发布的《个人信息出境安全评估办法（征求意见稿）》

2.3.3 赋予超级互联网平台守门人角色

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其进行监督，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。

2.4 明确管理责任部门及其职责

2.4.1 管理责任部门及其职责

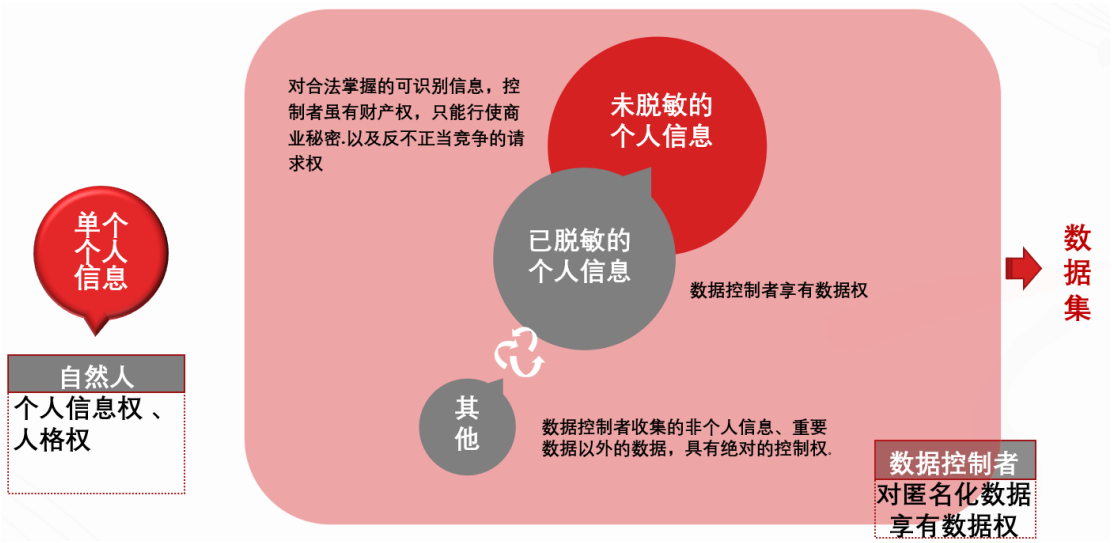


在中央层面，分国家网信部门的统筹协调角色以及国务院其他部门在各自职责范围的对口监管，中央和地方县级实行两级监管体制。监管职责的内容则主要体现为“宣传教育、指导、监督”，“对保护情况进行测评”“接受、处理举报和投诉”以及“调查、处理违法活动”等方面。

2.4.2 加大了惩处强度

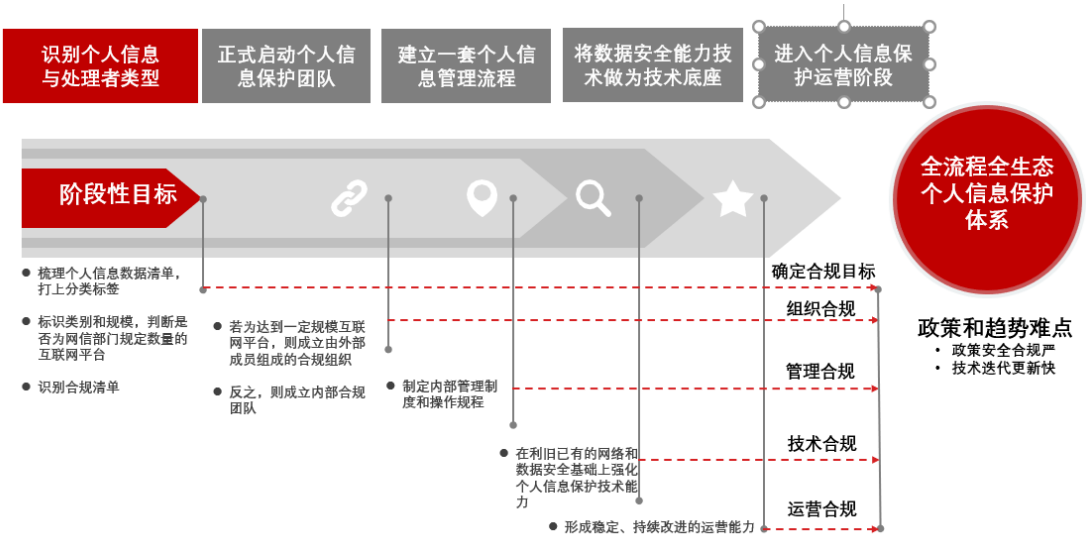
若个人信息处理者违反《个人信息保护法》规定，将会**由省级以上**履行个人信息保护职责的部门对企业和主管个人信息的个人进行处罚，情节严重的，没收违法所得，并处五千万元以下或者上一年度营业额百分之五罚款，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。相较于之前的所有的法律，可谓是最严的处罚，提高了企业的违规成本，起到了更强的警示作用。

3 企业合规路径



首先需明确数据安全与个人信息保护之间的关系，《数据安全法》是数据安全领域的基础法律，与《个人信息保护法》并行成为网络空间治理和数据保护的两驾马车，《数据安全法》负责规范数据处理活动、保障数据安全与促进数据开发利用，《个人信息保护法》提出以宪法为基础，**关乎人权**，负责个人信息权益、尊严和自由的保护，具有一般法和特别法的关系，一般数据处理活动要依据《数据安全法》，而**如果涉及个人数据的处理，则既要满足数安法的基础性规定，又要满足《个人保护法》的特殊性规定，匿名化处理的个人信息除外。**故企业可以将已有的数据安全能力作为基础，**以合规要求为抓手做好个人信息保护**，具体的路径包括识别个人信息和处理者自身的类型从而确认合规目标，启动个人信息保护团队，建立管理流程确定管控策略，通过对数据安全技术能力利旧，固化流程进入稳定的个人信息保护运营阶段，从而形成全流程全生态的个人信息保护体系。

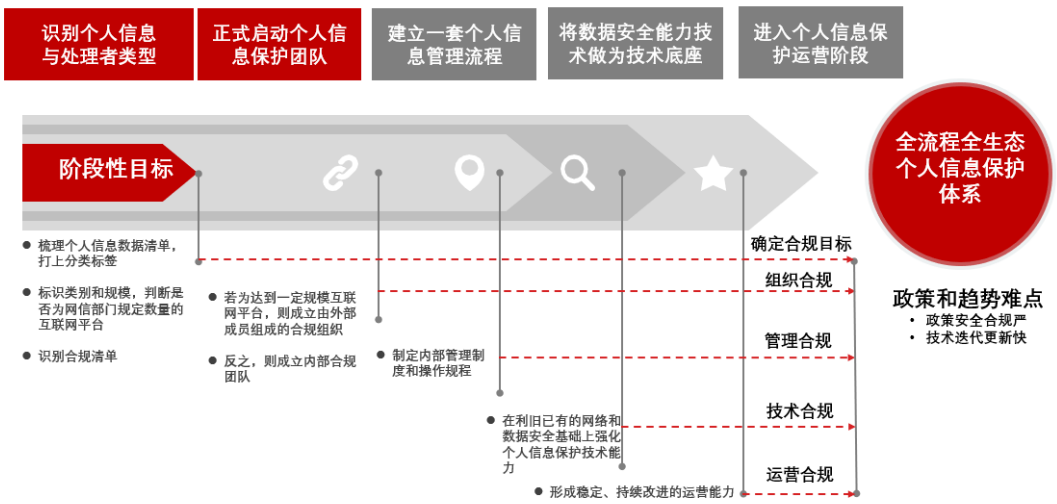
3.1 识别个人信息与处理者类型



在《数据安全法》中要求对数据进行分类分级保护，在《个人信息保护法》中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**在数据资产清单的基础上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。

同时也需确认个人信息的数据量，以判断是否达到了网信部门规定的个人信数据量的规模的，是否是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，从而判断自身需满足的合规要求及当前可能存在的问题，**形成《合规清单》、《负面清单》。**

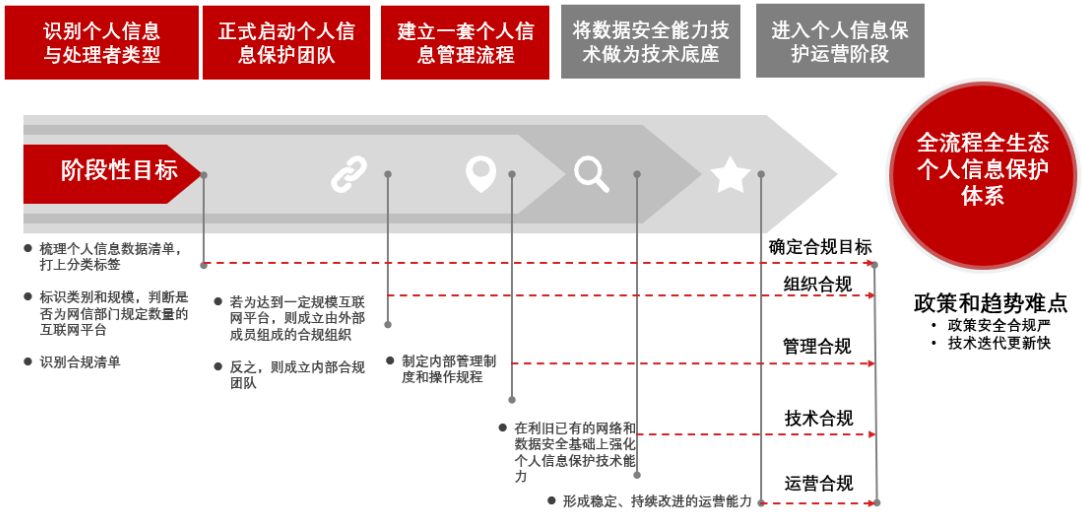
3.2 正式启动个人信息保护团队



企业应明确个人信息保护责任部门与人员，任命个人信息保护负责人和个人信息保护工作机构，个人信息保护负责人应由具有相关管理工作经历和个人信息保护专业知识的人员担任，参与有关个人信息处理活动的重要决策直接向企业主要负责人报告工作，具体可参照《信息技术 个人信息安全规范》第 11 章具体执行。必要时，**还需建立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。**

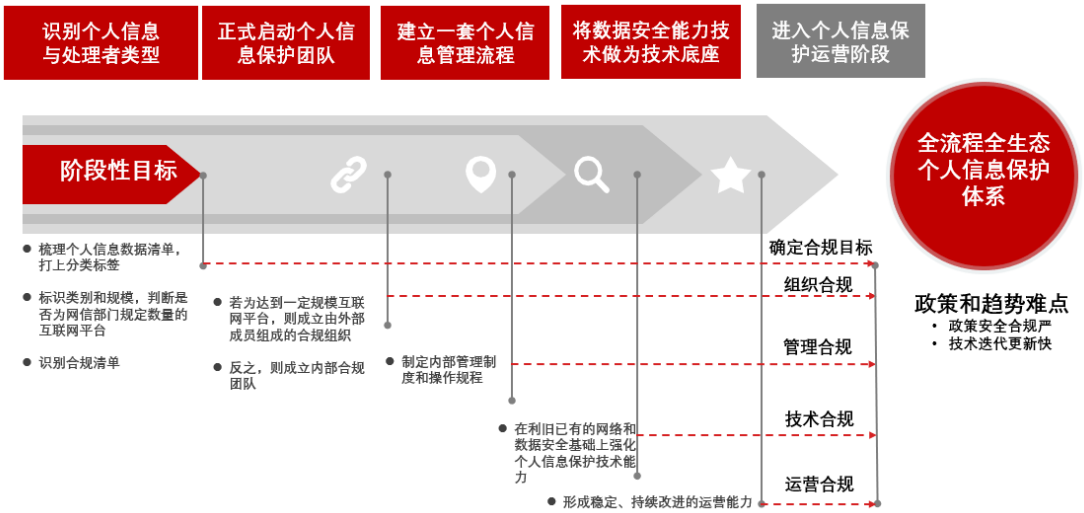
对于处理个人信息达到国家网信部门规定数量的个人信息处理者应指定专职个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

3.3 建立一套个人信息保护流程



制定适合于企业自身业务特点的管理要求，通过细化的操作规程，从而管控具体业务场景中针对个人信息的处理目的、处理方式、个人信息种类等安全风险和对个人信息主体权益的影响。可能包含**《个人信息保护管理办法》、《个人信息安全影响评估指南》、《个人信息安全事件应急管理规范》、《个人信息安全举报投诉管理规范》、《PII 全生命周期安全管理程序》、《隐私策略发布管理程序》、《PII 恢复工作规程》、《PII 主体利益维护指南》、《PII 去标识化操作规程》**等。

3.4 将数据安全能力作为技术底座



利用网络安全及数据安全防护产品，防范个人信息在个人信息处理活动中的

风险，具体情形如下：

收集阶段：采用**个人信息识别技术**、打上**个人信息种类标记**；

存储阶段：采用**加密、去标识化**等技术防范未授权的访问，定期进行**数据备份和恢复性测试**，同时也需注意个人信息**存储时间最小化**的问题；

使用阶段：采用**数据访问控制**等安全产品防范未授权的个人信息访问，采用**脱敏检查工具**，查验脱敏工作的有效性；定期进行**数据安全审计**，及时发现和处置数据非授权访问和异常操作；

加工阶段：进行自动化决策、定向分析时，对数据分析操作进行记录，以备对分析结果质量和可信性进行**数据溯源**；

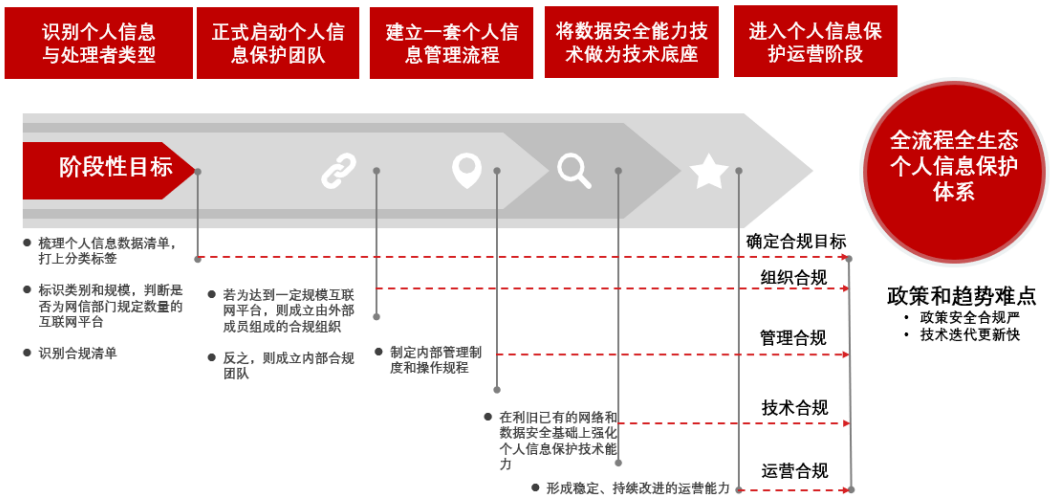
传输阶段：使用**加密、鉴别**的安全措施，采用**数据防泄漏产品**，防止个人信息外泄；

提供阶段：确保个人信息已做**好匿名化**处理，若需提供真实个人信息则需提前进行安全评估；

公开阶段：公开个人信息时采取**去标识化处**理等措施，并在合理区间内公开；

删除阶段：达成处理目的后，立即**删除或匿名化处理**，并进行**有效性验证**；

3.5 进入个人信息保护运营阶段

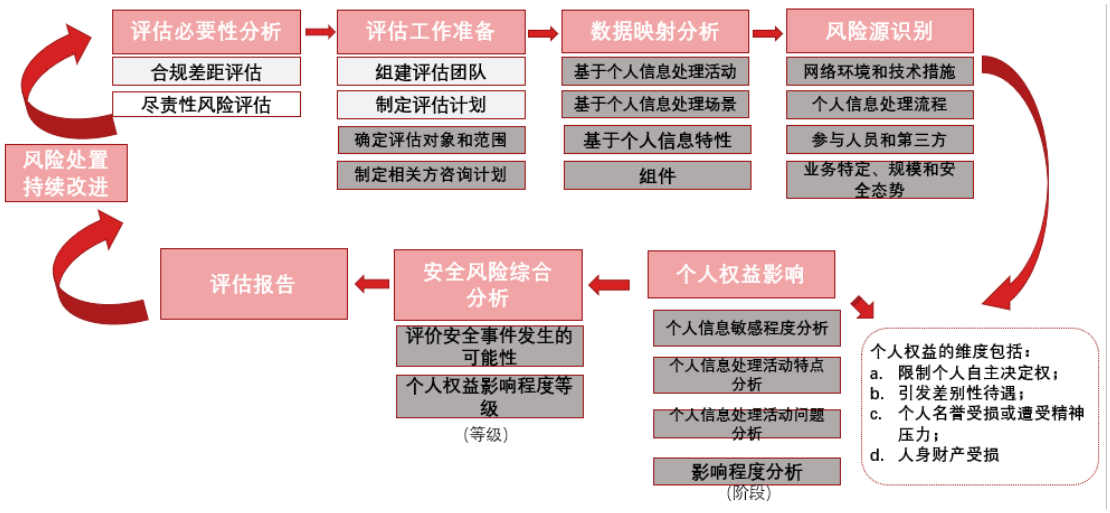


3.5.1 动态运营隐私条款

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、新增数据处理者等情况时，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。**

3.5.1 进行个人信息保护影响评估



在满足有下列情形之一的时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。具体可参考《个人信息安全影响评估指南》中相关要求。

3.5.2 合理确定个人信息处理的操作权限

通过良好的访问控制、账号权限管理、细颗粒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。**

3.5.3 定期对从业人员进行安全教育和培训

通过定期对相关岗位人员进行个人信息保护专项培训，并进行考核，确保相应的人员具备一定的安全意识和安全能力。

3.5.4 关注共同处理个人信息的风险

数据采集后的实际场景中，时常会出现有两个甚至多个数据控制者，《个人信息保护法》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**做好充足的资质审核、合作方安全管理审核**等工作，同时还应将各方责任落实到具体的法律文件当中，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。

3.5.5 关注委托他人处理个人信息的风险

“受委托方”与 “共同处理者”不同，委托方不具备数据的控制权，也不需要承担连带责任，**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**，且当合同不生效、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。

3.5.1 提高个人信息安全事件响应能力

制定适合自身业务场景的个人信息安全事件应急预案，并定期组织开展应急演练，提高个人信息安全事件的应急响应能力。在发生个人信息泄露、篡改、丢失、违规使用时，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、违规使用的信息种类、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）个人信息处理者的联系方式。

4 后续仍需持续关注

《个人信息保护》法现已发布，**但后续仍有很多具体事项需相关部门明确，我们也需持续关注**，如：

四十条要求：“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。”那**么规定的数量具体又是多少？可不进行安全评估的条件又有哪些？**

第五十八条要求："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……" **那么多大规模的个人信息处理者满足对应条件？**