千呼万唤始出来，一文读懂《个人信息保护法》亮点变革

作者：潘永建 | 杨迅 | 朱晓阳 | 邓梓珊 | 杨坚琪 | 胡鑫超

互联网时代，个人信息成为整个社会的关注焦点。随着个人信息保护问题步入“深水区”，个人信息保护立法也历经千锤百炼。继《网络安全法》《民法典》等对个人信息保护保护做出原则性规定后，个人信息保护单行法立法开始启动：2020 年 10 月公布《个人信息保护法(草案)》，2021 年 4 月公布《个人信息保护法(草案二次审议稿)》(以下简称“二审稿”)，2021 年 8 月 20 日，十三届全国人大常委会第三十次会议正式表决通过《个人信息保护法》(以下简称“个保法”)，将于 2021 年 11 月 1 日正式施行，结束了我国没有一部整体性、高位阶的个人信息保护立法的历史。本文将结合个保法较二审稿的修订亮点，对即将生效的《个人信息保护法》进行全方位重点解读。

内容速览：

- 个保法修订亮点
- 个人信息的定义有所变化
- 知情同意不再是处理个人信息的唯一合法基础
- 处理人脸信息应取得单独同意
- “大数据杀熟”不再有机可乘
- 进一步细化个人信息出境规则
- 新增个人信息可携权与侵权救济方式
- 个人信息违法行为处罚措施升级，设定企业和个人的“能力罚”
- 为个人信息主体维权提供便利

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

个保法修订亮点:

- 将劳动雇佣场景纳入无需获得同意的个人信息处理情形
- 不得利用用户画像进行“大数据杀熟”
- 处理个人敏感信息应取得“单独同意”
- 新增个人信息主体的“个人信息可携权”
- 明确自然人对其身后个人信息如何处理进行安排
- 将“基础性互联网平台服务”提供者修改为“重要互联网平台服务”提供者，并新增规则制定义务
- 将“下架应用”纳入处罚措施
- 对违法行为直接负责的人员将面临罚款+担任“董监高”的能力罚
- 明确消费者组织可以提起个人信息保护公益诉讼

1. 个人信息的定义有所变化

个保法第四条明确，个人信息是“以电子或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”。

基于《网络安全法》《民法典》等相关法律规范对个人信息所作的定义，个保法弥补了以往认定个人信息的漏洞，强调“可识别性”和“关联性”，即认定个人信息可采取两种方式，一种是从信息到个人，由信息本身的特殊性“识别”出特定自然人；第二种则是从个人到信息，如已知特定自然人，则与该自然人“相关”的所有信息均为个人信息。

实践中，判断个人信息是否具有可识别性、信息与自然人的关联程度的标准均尚未明晰。以近期司法实践为例，淘宝诉美景案确立了以数据接收方的识别能力作为判断可识别性的标准[1]；手机 MAC 地址信息因能够与其他信息结合获取手机用户的电话号码[2]，被法院认定为个人信息；好友列表信息因既能够识别到个人，又与已识别的个人相关[3]，亦被法院认定为个人信息。随着技术的更迭，各维度各渠道个人信息/标签信息的融合汇聚，数据接收方的数据来源、数据量、识别能力日益加强，个人信息的外延有不断扩大的趋势。数据处理者应对此保持清醒的认识，密切关注立法、执法及司法对于个人信息范围的认定，以确保准确界定自身的个人信息的义务。

2. 知情同意不再是处理个人信息的唯一合法基础

个保法第十三条列举了多项处理个人信息无需取得个人同意的情形，包括:

1) 为履行合同、实施人力资源管理所必需
2) 为履行法定义务所必需
3) 为应对突发公共卫生事件所必需
4) 为保护生命安全和财产安全所必需

[1] (2019)浙民申 1209 号。
[2] (2020)津 01 民终 3291 号。
[3] (2019)京 0491 民初 16142 号。

5) 为公共利益实施新闻报道等所必需
6) 在合理范围内处理已公开的个人信息

上述规定很大程度上放宽了个人信息处理的限制，突破了“告知同意”为核心的个人信息处理规则，意味着未来“知情同意”将不再是处理个人信息唯一的合法基础。

尽管企业最为关注的“在合理范围内处理已公开的个人信息”在一定程度上为企业利用个人信息提供了法律依据，但该项在实际应用时，仍然面临很大的挑战和不确定性，即“合理范围”难以界定，需要个案判断。根据《民法典》相关规定以及目前的司法和执法实践，判断“合理性”的关键是符合个人信息被公开时的预期用途。因此，企业仍需谨慎引用该例外情形处理个人信息。

此外，“为实施人力资源管理所必需”似乎便于雇主企业收集、使用员工个人信息，但企业仍应关注“人力资源管理所必需”的精准界定。例如员工个个人信息出境是否是“必需”，以及收集员工家属或其他紧急联系人的个人信息是否“必需”等。企业在处理员工个人信息时仍然需要遵守必要性原则，并对“为实施人力资源管理所必需”进行合理限缩解释。

3. 处理人脸信息应取得单独同意

个保法设专章对与人格尊严、人身财产安全直接相关的敏感个人信息进行详细规定。除生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息外，新增不满十四周岁未成年人的个人信息也属于敏感个人信息。基于“知情同意”原则，个保法第二十九条进一步要求处理敏感个人信息应取得个人的“**单独同意**”。

根据《信息安全技术 个人信息告知同意指南(征求意见稿)》：
“单独同意”是指通过“增强式告知”或“即时提示”等方式，单独向个人信息主体告知处理个人信息的目的、方式和范围、以及存储时间、安全措施等规则，并由个人信息主体**明示同意**(主动作出肯定性动作);
“增强式告知”，指采用个人信息主体不可绕过的方式(如弹窗等)向个人信息主体展示相关信息，以协助其作出是否授权同意的决定。

从“人脸识别第一案”，到“大爷戴头盔前往售楼处看房”，到 315 晚会“人脸识别系统”被曝光，作为敏感个人信息中社交属性最强、最容易采集的个人信息，人脸信息的收集利用备受争议。按照个保法第二十六条的要求，如以维护公共安全以外的目的在公共场所设置图像采集、人脸识别装置，应征得自然人(或者其监护人)的单独同意。个保法的这一规定与前段时间生效的《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》的要求相一致，且个保法限缩了使用目的。

企业确需出于其他目的收集处理人脸信息的，除设置显著的提示标识外，还应通过交互方式取得个人的明示同意，不应仅在隐私政策中笼统表述而不作单独说明。

4. “大数据杀熟”不再有机可乘

监管部门在近期 APP 违法违规专项整治行动中，发现大量 APP 存在违反必要原则，收集与提供的服务无关的个人信息。对此，个保法对企业处理个人信息的“必要性”进行专门规制，要求处理个人信息应与处理目的直接相关，收集范围应限于实现处理目的的最小范围，并应采取对个人权益影响最小的方式。随着个保法的落地，监管部门将参照《常见类型移动互联网应用程序必要个人信息范围规定》重点关注 APP 收集个人信息的“必要性”。

鉴于数据利用实践，通常“过度收集”仅是手段，而“滥用数据”才是目的，此次个保法对“自动化决策”作出专门限制，旨在直接打击愈来愈“猖獗”的“大数据杀熟”行为。按照规定，自动化决策应当事先进行个人信息保护影响评估；最关键的是，企业不得通过自动化决策对个人在交易价格等交易条件上实行不合理的差别待遇。同时，如利用自动化决策进行信息推送、商业营销，个人有权拒绝企业仅通过自动化决策的方式作出决定。

当然，企业对于个人信息的自动化决策算法往往极为保密，难以为个人信息主体所知。即便可以通过调查多个个人信息主体，使用不同设备等方式进行“验证”，但企业往往可以“供需关系”、“平台内第三方行为”等理由进行搪塞。因此，为更好地保护个人信息主体不受“大数据杀熟”的权利，法律对此应设置更为合理的举证责任及举证内容机制。

5. 进一步细化个人信息出境规则

根据个保法，个人信息出境将按照不同的个人信息处理者，实施不同类型的个人信息出境安全审查。具体而言:

(1) **关键信息基础设施运营者(CIIO)**原则上应将其在境内收集的个人信息储存在本地。确需向境外传输的，应当通过国家网信部门组织的安全评估;

(2) **一般的个人信息处理者**如处理信息未达到规定数量，通过专业机构的认证，或者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后，即可出境；如处理数量达到规定数量，则参照 CIIO 进行管理。

除上述程序外，企业对外提供个人信息，还需满足其他条件，包括:

(1) 履行告知义务;

(2) 获取单独同意;

(3) 事先进行风险评估;

(4) 采取必要措施保障境外处理活动达到个人信息保护标准。

此外，如外国司法或者执法机构要求企业提供存储于境内的个人信息，企业也应事先取得主管机关的批准。

6. 新增个人信息可携权与侵权救济方式

个保法第四章明确列举了个人在个人信息处理活动中的权利，包括知情权、决定权、限制和拒绝权、查阅权、复制权、更正权、删除权、撤回同意的权利。当自然人死亡时，其个人信息首先可以按照其生前的安排进行处理；没有特殊安排的，其近亲属可基于自身的合法正当利益行使查阅、复制、更正、删除死者相关个人信息的权利。此外，个保法借鉴欧盟的立法经验，增加了个人信息可携带权的规定。

对该等个人信息权利的保护，旨在解决现实中日益增多的因自然人去世引发的个人信息纠纷。此外，个保法借鉴欧盟的立法经验，增加了个人信息可携带权的规定。具体而言，当个人请求将其个人信息转移至其指定的个人信息处理者，只要符合国家网信部门规定的条件，企业即应当提供转移的途径。换言之，未来或许用户通过“一键转移”即可实现个人信息从一个平台转移至另一个平台。上述个人信息权利的保障机制将对企业设计产品和业务流程产生直接影响，同时也对不同企业所掌握的个人信息的类型、格式和结构做出了更高的要求，只有当相关的标准为足够多的企业所采取时，可携权才能真正地得以实现。

7. 个人信息违法行为处罚措施升级，设定企业和个人的“能力罚”

个保法承继了严厉惩罚个人信息违法行为的国际通行做法，加重了对侵犯个人信息行为的惩处力度。首先，与此前已采取的“通报批评→责令限期整改→下架处理”的 APP 整治手段保持一致，针对目前常见的 APP 违法违规收集使用个人信息的现象，**个保法专门设置了“责令暂停或终止提供服务”的处罚**。

此外，相较于《网络安全法》，对于“情节严重”的行为，违法企业可能被处以 5000 万元以下或者**上一年度营业额 5%以下罚款**。而相关责任人员不仅可能受到高达百万的罚款，还可能同时受到从业限制，在一定期限内无法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。如违法处理个人信息涉嫌犯罪，监管部门将同时移送公安机关处理。

尽管个保法对何种违法行为将落入“情节严重”的范围未提出明确标准，留待执法部门出台更细致的裁量规则。但整体而言，个保法设置的处罚全面覆盖了常见的违法行为，将精准打击各类违法主体，增加的处罚种类和加重的处罚力度都将大大增加企业的违法成本。

8. 为个人信息主体维权提供便利

在检察机关个人信息保护公益诉讼的实践基础上，个保法第七十条正式引入了个人信息保护公益诉讼制度。未来，当企业侵害众多个人的权益时，受侵害个人因取证难、成本高等问题放弃维权的现象将大大减少，检察机关、消费者组织和国家网信部门确定的组织将运用公益诉讼保障个人信息权益。值得注意的是，监管部门的介入不仅能够向违法者主张公益损害赔偿，还可能进一步依法追究违法者的行政和刑事责任。

此外，考虑到民事诉讼中个人通常举证能力有限，个保法第六十九条确立了侵害个人信息纠纷中的“过错推定责任”，当个人信息权益因个人信息处理活动受到侵害，需由个人信息处理者证明其没有过错，通过举证责任的转移实现对个人的倾向性保护。换言之，企业应有效证明自己通过完善的安全措施尽到个人信息保护义务，否则需承担损害赔偿责任。

结语

以往违法收集个人信息、滥用个人信息的违法成本极低，而由此带来的“流量变现”“海量用户画像”“精准营销(骚扰)”等业务却十分暴利。某些企业以身试法、屡试不爽，却给广大个人信息主体的正常生活乃至财产安全、生命安全造成了威胁，《个人信息保护法》的出台可以说是“千呼万唤始出来”。在这样的大背景下，企业处理和保护个人信息的实践不仅面临监管部门的执法高压，还将受到广泛的社会监督，个人信息合规势必成为企业合规建设的核心及要务。严格遵从《个人信息保护法》，对个人信息保护制度和实践进行整改和完善，已成为企业经营的“当务之急”，更是企业发展的“长久之计”。

囿于篇幅，本文仅简要列举《个人信息保护法》的重点内容，如需了解更多我们关于《个人信息保护法》的解读，请持续关注**“通力律师”公众号中的“数据合规”话题**。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市建国门北大街 8 号 华润大厦 4 楼 T: +86 10 8519 2266 F: +86 10 8519 2929	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野