LINKS Law Offices
通力律师事务所

上海
上海市银城中路 68 号
时代金融中心 16/19 楼
电话: +86 21 3135 8666
传真: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
电话: +86 10 8519 2266
传真: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话: +852 2592 1978
传真: +852 2868 0883

伦敦
1/F, 3 More London
Riverside, London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

通力法律评述 | 公司及并购
2020 年 2 月

疫情期间的个人信息保护——兼评《联防联控通知》

作者：杨迅 | 杨坚琪

为遏制新型冠状病毒肺炎疫情的发展，根据卫生健康主管部门的要求，各个企业也采取了对其员工和与其有直接接触的顾客(比如宾馆的入住人员)的防控措施，这些措施包括收集来自武汉或与武汉存在密切相关人员的个人信息。为促进被收集信息的安全利用，制止个人信息被滥用的可能性，中央网络安全和信息化委员会办公室颁布了《关于做好个人信息保护利用大数据支撑联防联控工作的通知》(**“《联防联控通知》”**)，对为疫情防控目的进行地个人信息收集提出信息安全方面的要求，进一步加强和细化了《网络安全法》下对个人信息收集使用的合法正当、知情同意、必要最少和安全权责原则。

一. 个人信息收集的“合法正当”基础

“合法正当”原则要求收集个人信息必须有合法的基础，且收集的手段必须正当。通常而言，“合法”地收集个人信息的基础包括：(1)依据法律规定，对个人信息进行收集；以及(2)基于一定的合同关系收集个人信息。

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

为对抗疫情，我国多部相关的法律法规要求卫生主管部门和专业机构了解公民的过往旅行信息、居住信息、密切接触者信息和健康信息等，公民个人也有义务提供该些信息。比如，《传染病防治法》第十二条要求：“在中华人民共和国领域内的一切单位和个人，必须接受疾病预防控制机构、医疗机构有关传染病的调查、检验、采集样本、隔离治疗等预防、控制措施，如实提供有关情况。”第三十一条：“任何单位和个人发现传染病病人或者疑似传染病病人时，应当及时向附近的疾病预防控制机构或者医疗机构报告。”可见，这些规定构成了为防控疫情目的收集有关个人信息的法律基础。

上述法律法规下的信息收集主体是政府机关，但是政府机关可以要求企事业单位配合开展信息收集工作。例如，上海市政府于 2020 年 1 月 27 日要求发布《上海市人民政府关于延迟本市企业复工和学校开学的通知》，其中明确要求“针对确因工作需要近期返沪的人员……所在单位要及时报告相关信息……”于是，企事业也就有了收集与防控疫情有关的个人信息的法律基础。

除法律法规和政府要求外，收集个人信息的合法基础也包括合同关系。企业与员工之间的劳动关系、企业与顾客之间的服务关系都是属于收集个人信息的合法基础。对于大多数企业而言，员工是生产经营的主体，如果有员工患有新型冠状病毒肺炎，或者已经是疑似患者或其密切接触者，可能会威胁企业其他员工的健康安全，进而对企业的生产经营产生重大影响。对于企业直接接触的顾客也是同样，对其将康状况的了解，也是保障业务持续的重要因素之一。因而，出于企业自身的利益，在疫情期间收集了解员工和直接接触的顾客的过往旅行史、密切接触史和健康信息是有合法基础的。

二. 收集个人信息的“知情同意”要求

根据《网络安全法》的规定，“知情同意”原则要求：个人信息的收集者应当向个人信息主体(比如企业员工或者顾客)告知其收集、使用个人信息的“目的、方式和范围”以及拒绝收集的后果，并获取其对收集其个人信息的同意。换而言之，只有在个人信息主体清楚、明白地知悉相关个人信息收集和使用规则，并在给出“同意”后，个人信息的收集者才能够收集、使用他人的个人信息。那么这是否意味着，在中国法下，任何个人信息的收集都必须经过信息主体“知情同意”呢？

虽然《网络安全法》没有明确给出“知情同意”要求的例外，《信息安全技术-个人信息安全规范》(“**《个人信息规范》**”)在“知情同意”的原则下，提出了可能不经过信息主体“知情同意”而收集个人信息的场景。典型的例子是，根据《个人信息规范》第 5.4 条，在“与公共安全、公共卫生、重大公共利益直接相关的”的情形中，个人信息控制者收集、使用个人信息可以无需征得个人信息主体的授权同意，直接“收集、使用”个人信息。换而言之，如果是为了保护“与公共安全、公共卫生、重大公共利益”的需要，个人信息主体没有“拒绝”的权利；相反，即使没有他们的“同意”，政府机关、授权机关和履行法定义务的主体(包括按照法律法规和政府指令要求收集个人信息的企业)也有权收集法律规定的个人信息。

《联防联控通知》明确指出：除国务院卫生健康部门依法授权机构外，“其他任何单位和个人不得以疫情防控、疾病防治为由，未经被收集者同意收集使用个人信息。”换而言之，如果是获得依法授权的，那么为防疫目的收集个人信息，就不需要得到信息主体的同意。

值得注意的是，虽然《个人信息规范》“豁免”了个人信息收集时的“同意”要求，但是并没有明确豁免“知情”原则的要求。也就是说，哪怕基于法定要求的个人信息收集，如果可行，也需要尽可能充分和明晰地披露“目的、方式和范围”。

三. 收集使用个人信息的“必要最小”原则

为履行防控疫情的法定义务，抑或出于保证员工健康安全，并不意味着主管部门(或者其委托的机构)或企业可以无限制地索取个人信息。收集、使用个人信息必须要遵守“必要最小”原则，即，收集信息的范围应仅限于实现收集的目的的必要范围内，并且个人信息的保存期限也不得超过必要使用的期间。《联防联控通知》也指出：“收集联防联控所必需的个人信息应……坚持最小范围原则，收集对象原则上限于确诊者、疑似者、密切接触者等重点人群，一般不针对特定地区的所有人群，防止形成对特定地域人群的事实上歧视”，并且“为疫情防控、疾病防治收集的个人信息，不得用于其他用途”。具体而言：

第一，从收集对象而言，仅限于“确诊者、疑似者、密切接触者等重点人群”，而不是所有人，也不是对某一地区人员普遍性的收集。收集个人信息的对象要符合收集的目的。

第二，从范围上来讲，以防控疫情为目的的合理个人信息范围应限定在一定期限内的旅行史、饮食史、接触史等与预防、控制疾病直接相关的信息。如果是与疫情无关的其他信息，比如财产信息、宗教信息或者学历信息等，就不应当列入个人信息收集范围内。

第三，从使用目的上说，基于履行法定义务、医疗、防控目的的个人信息的收集和使用，应当限于该目的使用个人信息，而不得为其他目的使用，比如为推销药品、卫生用品而构筑潜在用户信息库等商业目的进行使用。

第四，从使用方式看，个人信息的处理、利用和披露不能超过法定或信息主体同意的范围，且不得与其他渠道的个人信息进行混用。比如企业为防控疫情而收集的信息，只能告知必要的处理信息的个别人员(比如人事部门的专员)，为保证其提供的服务安全所收集的信息只能由相关业务部门指定专员处理，不能向没有必要知悉的其他员工披露。

第五，从保存期限上说，基于疫情原因收集的个人信息，收集者应当在疫情结束后及时删除(法律要求和允许保留的除外)，或者对这些个人信息采取去个性化措施。

四. 对外提供个人信息的限制

基于收集使用个人信息的“最小必要”原则，企业只能在最小必要的范围内披露个人信息，不可以超过必要限度，例如向第三方提供或向公众披露个人信息，尤其是可能与疾病相关的个人信息。

有多部法律都对个人信息的披露作出限制。《网络安全法》第四十二条要求，未经个人同意，网络运营者不得向第三人提供其收集的个人信息；《传染病防治法》第十二条要求，疾病预防控制机构、医疗机构不得泄露涉及个人隐私的有关信息、资料。为了控制疫情，交通运输部特别下发了《关于统筹做好疫情防控和交通运输保障工作的紧急通知》，其中也特别要求“要依法严格保护个人隐私和个人信息安全，除因疫情防控需要，向卫生健康等部门提供外乘客信息外，不得向其他机构、组织或者个人泄露有关信息、不得擅自在互联网散播。”

针对近期政府有关主管部门泄漏确诊病人和疑似病人个人信息的事件(比如湖南省益阳市赫山区卫生健康局某副局长涉嫌将新冠病毒患者及其亲属 11 人的个人信息不当披露)，《联防联控通知》明确指出：“任何单位和个人未经被收集者同意，不得公开姓名、年龄、身份证号码、电话号码、家庭住址等个人信息，因联防联控工作需要，且经过脱敏处理的除外。”实际上，法律所要求的，为疫情防控目的而进行的个人信息收集和处理应当仅限于政府内部。未经被收集者的同意或者法律要求，其也不得向公众公开披露个人信息。

同时，国家鼓励对疫情防控有关的大数据的运用。比如，《联防联控通知》“鼓励有能力的企业在有关部门的指导下，积极利用大数据，分析预测确诊者、疑似者、密切接触者等重点人群的流动情况，为联防联控工作提供大数据支持。”也就是说，法律并不禁止政府或者有关部门充分利用企业的信息处理能力以支持疫情的防控，但是原则上应以匿名化的信息为主。

对企业而言，当企业获取员工或者顾客的个人信息时，其应当采取必要的技术手段和管理手段防止信息的不正当泄露，包括制止主动的信息披露，也包括由于过失导致信息泄露。

五. 收集使用个人信息的安全原则

对于个人信息的收集者而言，在完成收集个人信息之后，其有义务采取必要的措施保护个人信息安全。

根据《网络安全法》的要求，个人信息的收集主体应当采取“技术措施”和“其他必要措施”，以防止可能的信息泄露、毁损或者丢失。《联防联控通知》也要求“收集或掌握个人信息的机构要对个人信息的安全保护负责，采取严格的管理和技术防护措施，防止被窃取、被泄露。”

从管理措施的角度来看，主要包括制定隐私政策、制定信息安全体系战略、灾备政策等，以及针对不同的人员设定不同的权限和访问限制等；从技术措施的角度来看，应当根据相应的等级保护要求，采取必要的物理访问限制措施、加密措施以及在各个层面部署安全分析工具和防火墙，以维护个人信息及其相关的数据库的安全性。考虑到“等保 2.0”已经全面实施，可以参考《GB-T 22239-2019-信息安全技术-网络安全等级保护基本要求》等标准对于企业已经采取的安全措施进行核查。

此外，如果企业能够完成相应的认证，例如 ISO/IEC 27001:2013 信息安全管理体系认证或者 ISO/IEC 29151:2017 个人身份信息保护实践指南认证，那么这也无疑是对于安全措施有效性的强有力的证明。

总结

1. 对企业而言，可以依法或者基于员工和个人顾客的同意而收集防控疫情目的的个人信息。
2. 企业自行收集信息的，收集信息的范围限于以防控疫情有关的必要信息，并且应当充分披露信息收集的目的、方式和范围。
3. 企业需要自行储存和使用个人信息的，应当建立与之相适应的个人信息保存、使用和安全政策，防止信息泄露，仅向必须知晓的员工披露该些信息。
4. 信息收集使用的目的已经达到的，或者信息收集的目的不再适用的(如疫情结束)，所收集的信息应当销毁，或者对其进行匿名化处理。

如您希望就相关问题进一步交流，请联系：

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	香港	伦敦
T: +86 21 3135 8666 F: +86 21 3135 8600	T: +86 10 8519 2266 F: +86 10 8519 2929	T: +852 2592 1978 F: +852 2868 0883	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