Legal Insight | 法律洞察

20 March 2020
202003/006

Inside this issue:

Personal Data Protection during COVID-19 Control and Prevention

Throughout the course of intensive epidemic response, large amounts of personal data (such as names, mobile phone numbers, residence addresses, etc.) have been leaked, causing great distress and harm to all involved. On one hand, individual citizens are disturbed by the collection of their personal information organized by communities, employers and authorities, because they do not know whether the information they submitted will be protected properly. On the other hand, enterprises are engaged in a balancing act, as they must implement epidemic prevention measures and control obligations for production resumption, but must also be careful to avoid overstepping the red line of personal information protection. In early February, with regards to personal data concerns and epidemic response measures, the Cyberspace Administration of China issued the "Circular on Ensuring Effective Personal Information Protection and Utilization of Big Data to Support Joint Efforts for Epidemic Prevention and Control" (hereinafter referred to as Circular) .

Below, we briefly detail the matters related to the collection and utilization of personal information during the epidemic. Enterprises that abide by data and epidemic regulations will be able to endure difficulties without violations of any regulations.

I. Definition of Personal Information

Defined in "Personal Information Security Specification", personal information refers to all information which can be used independently or in combination with other information to identify a natural person or uncover the activities of a natural person. Personal information that may cause harm to personal or property security, or is likely to result in damage to an individual's personal reputation or physical or mental health or give rise to discriminatory treatment, once it is leaked, unlawfully provided or abused, is called "personal sensitive information" and requires a higher level of protection.

Although the "Personal Information Security Specification" enumerated types of "personal sensitive information", it can be ascertained from its scenario-based definition that what kind of data will be considered as "personal sensitive information" requires the personal infor-

mation controller's confirmations according to the consequences of information release. For example, leaking the personal information of returnees from Wuhan, diagnosed patients of COVID-19, suspected patients and close contacts may lead to harassment, abuse, threats and other illegal acts, thus "very likely to give rise to damages to personal(including family members) reputation, physical and mental health, as well as discriminatory treatment". Therefore, the controller is required to protect the personal information of these specific groups in accordance with the standards applying to "personal sensitive information".

II. Subjects of and Legal Basis for Personal Information Collection for Epidemic Prevention and Control

According to the "Cybersecurity Law of the People's Republic of China" and the corresponding national standard "Personal Information Security Specification", the general principle for collecting personal information is "notification from controllers & consent of the personal information subjects", especially for sensitive personal information, which may only be collected with explicit consent.

On January 20, 2020, the National Health Commission issued Announcement No. 1 to incorporate COVID-19 into Class B of infectious diseases as stipulated in "the Law of the People's Republic of China on Prevention and Treatment of Infectious Diseases". Furthermore, the Commission adopted Class A measures for the prevention and control of infectious diseases. Subsequently, some provinces, autonomous regions and municipalities initiated first-level responses under the pretext of a major public health emergency. Therefore, all government departments and entities are taking corresponding measures in accordance with relevant laws and regulations such as the "Prevention and Treatment of Infectious Diseases Law" and the "Regulation on Responses to Public Health Emergencies" policy. Accordingly, disease prevention and control institutions as well as medical agencies are obligated to report epidemic related cases[1]. In addition, every entity or individual is obligated to cooperate with relevant state organs in the prevention and control of infectious diseases, which includes investigations and information collection related to the infectious disease, "No entity or individual may conceal, delay the report, or make a false report or hint any other person to conceal, delay the report, or make a false report of any emergency[2]". Therefore, the people's government may authorize departments, institutions, organizations and individuals besides public health administrative institutions, disease prevention and control institutions and medical institutions to collect and analyze personal information related to epidemic in response to public health emergencies.

As special laws prevail over general laws, the epidemic-related collection of personal information on the basis of the " Prevention and Treatment of Infectious Diseases Law" and the "Regulation on Responses to Public Health Emergencies" can occur without the related parties' consent. In addition, by reference to the "Personal Information Security Specification", the collection of data "related to the fulfillment of personal information controllers' obligations under laws and regulations"[3] or "directly related to public safety, health safety and major public interests" does not require the subject's authorization and consent. On January 20, 2020, following the National Health Commission's issue of Announcement No. 1, the National Information Security Standardization Technical Committee promulgated the "Information Security Technology — Guidelines for Personal Information Notices and Consent (Draft for comment)", which ruled that data collection measures related to "strengthening the prevention and control of specific epidemics which can cause human infections at ports, sampling the suspected case to conduct pathogen monitoring and registering his/her personal information in detail, etc." do not require the subject's consent.

Based on the above analysis, we can more clearly understand Article 1 of the Circular: Any entity or individual other than an institution authorized by State Council's health department

in accordance with the "Cybersecurity Law", the "Law on Prevention and Treatment of Infectious Diseases" and the "Regulation on Responses to Public Health Emergencies" shall not collect or use personal information without the consent of the persons whose information is to be collected on the grounds of epidemic prevention and control or disease treatment. Enterprises may collect personal data related to the epidemic situation as required by the local Centers for Disease Control and the people's government without the subject's consent, however, it is highly recommended that enterprises notify relevant personnel of the purpose, collection method, scope, security measure, storage period, etc. of the collected information.

III. Requirement to Comply with Relevant Protection Regulations while Collecting Personal Information for Epidemic Prevention and Control

The collection of personal data related to epidemic prevention and control by authorized institutions in accordance with the law does not require the consent of the information subject. However, these institutions' are not relieved of their responsibility and obligation to protect collected personal information.

1. Principle of Necessity and Minimization

Article 2 of the Circular, "Personal information necessary for epidemic prevention and control shall be collected by reference to the national standard 'Personal Information Security Specification', in adherence to the minimum scope principle. Collection targets shall be limited to key groups such as confirmed patients, suspected patients, and close contacts. The population of a particular region shall not be targeted in general, so as to prevent de facto discrimination against specific groups."

2. Prohibition of Changes in the Purpose and Utilization of the Collection

Article 3 of the Circular states that "Personal information collected for epidemic prevention and control and disease prevention and treatment shall not be used for any other purpose. No entity or individual may, without the consent of the personal information subjects, disclose their personal information such as name, age, identification number, phone number, and home address to the public, unless anonymized as necessary for joint prevention and control". Collected personal data shall not be used for purposes other than epidemic prevention and control; and even when it is used for epidemic prevention and control, it must be anonymized. In addition, when the epidemic ceases to exist, the stored personal information shall be deleted in accordance with relevant regulations.

3. Take Strict Leak Prevention Management and Technical Measures

Article 4 of the Circular states that "An institution that collects or is in possession of personal information shall be responsible for the security of personal information and adopt strict management and technical protection measures to prevent theft and divulgence". Policies guaranteeing the protection of personal data hold for the data's entire life cycle, including collection, use, transmission, transfer, sharing, storage, deletion, etc. Therefore, any person or entity that may obtain or access personal information under the auspices of epidemic control must uphold their obligation to prevent data leakage, abuse and loss. The personal information controller shall formulate strict access control measures in order to protect personal information through technical measures such as encryption, and to defend database auditing from attack, theft, abuse and leakage. Enterprises can take this opportunity to investigate their network information systems and internal data management for loopholes. Precaution is best, when preparing for personal information protection and network security issues brought by remote collaboration and office networks.

[1] Article 12 of “ Law of the People's Republic of China on Prevention and Treatment of Infectious Diseases” :
All units and individuals within the territory of the People's Republic of China shall accept the preventive and control measures taken by disease prevention and control institutions and medical agencies for investigation, testing, collection of samples of infectious diseases and for isolated treatment of such diseases, and they shall provide truthful information about the diseases. Disease prevention and control institutions and medical agencies shall not divulge any information or materials relating to personal privacy.
Article 31 of “ Law of the People's Republic of China on Prevention and Treatment of Infectious Diseases” :
When any unit or individual finds an infectious disease patient or a suspected one, they shall promptly report to the nearby disease prevention and control institution or medical agency.

[2] Article 21 of " Regulation on Responses to Public Health Emergencies " :
No entity or individual may conceal, delay the report or make a false report or hint any other person to conceal, delay the report or make a false report of any emergency.

[3] Art. 5.6 a) of “GBT 35273-2020 Personal Information Security Specification”.

疫情防控中的个人信息保护合规要点

在社会各界积极应对疫情的过程中，各地查处了多起姓名、手机号码、户籍地址等个人信息泄露事件，这些事件给相关人员的生活造成了极大的困扰和伤害。一方面，作为公民个体因被社区、单位收集个人信息而惴惴不安，不知道把个人信息交出去是否安全。另一方面，作为企业方，既要落实疫情防控义务有序复工，又不能踩了个人信息保护的红线，也可谓如履薄冰。面对疫情防控中个人信息收集使用的复杂情况，2月初中央网信办公布了《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》（以下简称“《通知》”）。

在此，我们对疫情中个人信息收集使用的相关事项进行简单梳理，希望帮助企业合法合规地渡过困难时期。

一、个人信息的定义

在《GBT 35273-2020个人信息安全规范》（以下简称“《个人信息安全规范》”）中，个人信息是指能够单独或者与其他信息结合识别特定自然人身份或反映特定自然人活动情况的各种信息。其中一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息称为个人敏感信息，需要更高级别的保护。

虽然《个人信息安全规范》对个人敏感信息也进行了列举，但通过其场景式的定义可以看出，何种个人信息会被认定为个人敏感信息，需要个人信息控制者在特定的场景中根据损害的后果进行逐一判断的。以武汉返乡人员、新冠肺炎确诊患者、疑似病例及密切接触者的个人信息为例，此类人员的姓名、手机号码、家庭住址等信息一旦泄露，极易引发针对该人群的骚扰、谩骂、威胁等违法行为，从而“极易导致个人（包括家人）名誉、身心健康受到损害或歧视性待遇”。因此需要个人信息控制者将该群体的个人信息按照“个人敏感信息”的标准进行保护。

二、为疫情防控有权收集个人信息的主体及法律依据

根据《中华人民共和国网络安全法》及相应国标《个人信息安全规范》，收集个人信息的一般原则是告知+同意，尤其是个人敏感信息，应以征得明示同意作为收集的前提。

2020年1月20日，国家卫健委发布1号公告，将新型冠状病毒感染的肺炎纳入《中华人民共和国传染病防治法》规定的乙类传染病，并采取甲类传染病的预防、控制措施。随后各省、自治区、直辖市启动重大突发公共卫生事件一级响应。因此，各政府部门、单位应按照《中华人民共和国传染病防治法》、《突发公共卫生事件应急条例》等相关法律规定采取相应措施。其中，为疫情管控，疾病预防控制机构、医疗机构具有相应的疫情报告义务[1]。另外，任何机构和个人有义务配合国家有关机关防控传染病有关的工作，这其中也包括与传染病有关的调查和信息采集，“任何单位和个人不得以任何理由予以拒绝”[2]。因此可以理解为人民政府在应对突发事件时，可以授权卫生行政机构、疾病预防控制机构和医疗机构之外的部门、机构、组织、个人，对信息进行收集分析。

由于特别法优于一般法，因此根据《中华人民共和国传染病防治法》、《突发公共卫生事件应急条例》授权收集与疫情防控有关的个人信息可免于征得当事人的同意。《个人信息安全规范》中也规定收集“与个人信息控制者履行法律法规规定的义

务相关的”以及“与公共安全、卫生安全、重大公共利益直接相关的”个人信息无需征得个人信息主体的授权同意。在2020年1月20日国家卫健委发布1号公告的当天，全国信息安全标准化技术委员会公布了《信息安全技术个人信息告知同意指南（征求意见稿）》，其中明确列举“例如加强口岸防控人感染特定流感疫情，对疑似病例人员采样进行病原体监测，详细登记其个人信息等”不必征得信息主体同意。

基于上述分析，我们可以更加清晰地理解《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》第1条“除国务院卫生健康部门依据《中华人民共和国网络安全法》《中华人民共和国传染病防治法》《突发公共卫生事件应急条例》授权的机构外，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。”各企业根据当地疾控中心、人民政府要求收集本单位与疫情相关的个人信息可以不需要征得信息主体的同意，但仍建议企业履行告知义务，通过书面材料告知相关人员收集信息的目的、方式、范围以及保密措施、存储期限等。

三、为疫情防控收集个人信息仍需遵守相关保护规定

依法被授权的机构收集与疫情防控相关的个人信息无需征得信息主体的同意，但并不免除其保护所收集的个人信息的责任和义务。

1、必要性、最小化原则

《通知》第2条：“收集联防联控所必需的个人信息应参照国家标准《个人信息安全规范》，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。”

2、不得改变收集目的和用途

《通知》第3条：“为疫情防控、疾病防治收集的个人信息，不得用于其他用途。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。”首先，收集的个人信息不能用于疫情防控以外的用途；即使用于防控目的，也应进行脱敏处理。另外，疫情防控目的消失后，应将存储的个人信息按规定予以删除。

3、采取严格的防泄漏管理和技术措施

《通知》第4条：“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。”个人信息保护贯穿数据的全生命周期（收集、使用、传输、转让、共享、存储、删除等），因此在疫情防控中任何可以获取、接触个人信息的人员和单位都有防止数据泄露、滥用、丢失的义务。作为个人信息控制者，应制定严密的访问控制措施，通过加密、数据库审计等技术手段对个人信息予以保护，防攻击、防窃取、防滥用、防泄露。企业可以借此机会，对自己的网络信息系统和内部数据管理制度进行摸底排查，围堵漏洞，防微杜渐，从而对之后网络办公、远程协作带来的个人信息保护和网络安全挑战未雨绸缪，做到有备无患、游刃有余。

---

[1]《中华人民共和国传染病防治法》第十二条：
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。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。
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。

[2]《突发公共卫生事件应急条例》第三章 报告与信息发布
第二十一条：
任何单位和个人对突发事件，不得隐瞒、缓报、谎报或者授意他人隐瞒、缓报、谎报。

远程办公安全防护指南 / Guideline on Remote Working Security

2020年3月13日全国信息安全标准化技术委员会秘书处发布了《网络安全标准实践指南——远程办公安全防护》（以下简称“《安全防护指南》”），为部分企业的“远程办公”、“数据上云”、“数字化转型”提供安全操作指南。

为方便阅读查询，现将《安全防护指南》中远程办公需注意的风险点归纳如下，供正在使用或拟实行远程办公的企业自查：

风险	原因
1. 远程办公系统风险	
	系统安全功能不完备，系统自身安全漏洞，不合适的安全配置等。
2. 数据安全风险	
数据泄露	数据访问权限设置不合理，远程办公系统自身安全漏洞，实行远程办公企业员工等用户的不当操作。
数据非法访问	实行远程办公的企业若使用云计算平台，可能失去对数据的直接管理和控制能力。
3. 设备风险	
可能将权限滥用、数据泄露风险引入远程办公企业内部网络	远程办公设备，特别是实行远程办公的企业员工等用户的自有设备，在接入远程办公系统时，由于未安装或及时更新安全防护软件，未启用适当的安全策略，被植入恶意软件等。
4. 个人信息保护风险	
被滥采、滥用和泄露的风险	远程办公系统的部分功能（例如，企业通信录、健康情况汇总、活动轨迹填报等），可能收集、存储企业员工等用户的个人信息（例如，姓名、电话、位置信息、身份证件号码、生物特征识别数据等）。
5. 网络通信风险	
通信中断，通信数据被篡改、被窃听的风险	企业员工等用户和远程办公系统通常利用公用网络进行通信。
办公活动难以进行	远程办公系统可能遭受恶意攻击（例如，分布式拒绝服务攻击等）。
6. 环境风险	
网络入侵和通信中断风险	远程办公通常在居家环境或公共场所进行。居家环境中，家用网络设备安全防护能力和网络通信保障能力较弱。
设备接入不安全网络、数据被窃取、设备丢失或被盗等风险	公共场所中网络环境和人员组成复杂。
7. 业务连续性风险	
增加了远程办公企业关键业务、高风险业务的安全风险	远程办公系统负载能力、访问控制措施、容灾备份、应急能力等方面不足。
8. 人员风险	
远程办公企业业务系统的恶意攻击	企业员工等用户可能由于安全意识缺失或未严格遵守企业的管理要求，引入安全风险，例如，将设备、账号与他人共享。
身份仿冒	企业员工等用户可能采用弱口令。

针对上述风险，实行远程办公的企业可以从管理、技术两大方面采取以下安全措施：

1 管理要求	1.1. 远程办公需求分析	
		企业应对业务、数据、业务系统进行安全风险分析，明确可用于远程办公的业务、数据和业务系统，以及相关安全需求。
	1.2. 远程办公系统选择	
		企业作为采购方 a）应重点考虑供应方的安全能力，包括但不限于安全开发运维、数据保护、个人信息保护等方面； b）应充分评估远程办公系统的安全性，按照下述安全要求选用远程办公系统，重点考虑远程办公系统与网络安全相关标准的符合性、数据存储位置、弹性扩容能力等； c）宜选取通过云计算服务安全评估的云计算平台，用于部署远程办公系统。
	1.3. 运维管理	
		实行远程办公的企业 a）应指定专门人员或团队负责远程办公安全； b）应开展远程办公系统配置管理，对安全策略、数据存储方法、身份鉴别和访问控制措施的变更等进行管理； c）应制定远程办公安全事件应急响应流程以及应急预案，定期开展应急预案演练； d）应根据业务和数据的重要性，制定备份与恢复策略； e）应要求供应方提供运维服务，例如，在线技术支撑、应急响应等，保障远程办公系统稳定运行。
	1.4. 管理制度	
		实行远程办公的企业 a）应制定远程办公安全管理制度，内容包括但不限于办公环境安全、数据安全、设备安全、个人信息保护、安全配置、通信安全、备份与恢复安全等； b）应制定远程办公安全操作细则，定期开展远程办公安全教育和培训，提升用户安全意识。
2 技术要求	2.1. 远程办公系统安全	
	2.1.1 服务端安全	系统安全要求 企业采用的远程办公系统应满足GB/T 22239 《信息安全技术网络安全等级保护基本要求》、GB/T 31168《信息安全技术云计算服务安全能力要求》、GB/T 35273《信息安全技术个人信息安全规范》的相关要求。
		在线会议安全 远程办公系统具备在线会议功能的： a）应具备身份鉴别功能，仅授权人员可以参加在线会议； b）会议管理员应能够设置参会用户权限； c）应支持加密方式存储、传输会议材料； d）在会议期间，宜提供参会人员关闭音频、视频设备的功能。
		即时通信安全 远程办公系统具备即时通信功能的： a）应加密存储即时通信消息； b）应提供账号管理、即时通信消息群成员的安全设置等功能； c）宜提供用户撤回即时通信消息的功能。
		文档协作安全 远程办公系统具备文档协作功能的： a）应支持加密方式对在线协作文档进行传输、存储； b）应提供操作审计功能，对重要操作（例如，文档的删除、复制等）进行记录； c）应在审计记录中包含账号、操作等信息；

		d）应具备文档内容防泄漏功能，例如，文档加密等； e）文档分享链接应仅对授权用户可用； f）文档分享链接宜根据分享范围进行控制，例如，限制访问人员等； g）宜提供文档数据恢复功能； h）宜对文档操作进行权限控制。
		接入安全 远程办公系统具备功能扩展模块的： a）应在接入远程办公系统前进行安全审核，例如，漏洞修复情况审核、内容安全审核； b）应具备身份验证、权限管理、输入检验、文件操作管理、数据加密等安全措施； c）在访问使用方的敏感数据前，应获得授权。
	2.1.2. 企业客户端安全	应用程序安全 远程办公系统的应用程序： a）应具备运行环境安全和程序完整性检测功能，例如，防篡改检测、模拟器检测等； b）应使用安全加固措施，例如，防止反编译、重打包等； c）应对使用过程中产生的数据（包括但不限于数据文件、日志文件、数据库文件、配置文件、密钥文件等）进行保护，例如，使用加密存储、安全沙箱等技术； d）应保护身份鉴别信息，例如，使用设备登陆检测等技术； e）应使用安全协议，例如，传输层安全协议（TLS）、因特网安全协议（IPSec）等，保护传输的保密性和完整性； f）应具备权限管理功能，允许使用方和用户根据远程办公需求调整权限； g）宜使用多因素鉴别方法对用户身份进行鉴别； h）宜具备信息防窃取和数据溯源措施； i）宜使用安全组件，例如，安全键盘等。
		浏览器应用安全 远程办公系统的浏览器： a）应使用安全的浏览器内核，避免已知漏洞被利用； b）应具备恶意网址的识别和拦截能力； c）宜具备用户名、Cookie、缓存的加密功能； d）宜具备浏览器插件、扩展的黑名单和白名单机制，防止恶意插件、扩展的安装、加载和运行。
	2.2. 访问控制	
		实行远程办公的企业： a）应建立适用于远程办公的访问控制机制，包括审核用户权限申请、定期审核用户权限、及时清除过期权限等； b）应对用户开放远程办公所需的最小权限，禁止用户账号共享。
	2.3. 业务系统安全	
		实行远程办公的企业： a）应划分业务安全域，对不同业务安全域进行隔离； b）应统一配置远程办公业务，最小化开放业务所需的服务和端口； c）应维护业务系统安全基线，确保相关安全补丁及时更新； d）宜持续对访问行为进行监控和分析，识别并及时阻断恶意用户和行为。

	2.4. 数据安全	
		实行远程办公的企业： a）应对数据进行分类分级； b）宜设置数据防泄漏策略； c）宜限制向用户自有设备传输使用方敏感数据； d）宜提供数据销毁方案。
	2.5. 个人信息保护	
		使用方应按照GB/T 35273《信息安全技术个人信息安全规范》要求保护个人信息。
	2.6. 通信安全	
		实行远程办公的企业： a）应使用安全协议，例如，传输层安全协议（TLS）、因特网安全协议（IPSec）等，保护业务系统传输的保密性和完整性； b）宜在通信过程中对设备的安全性进行持续验证。
	2.7. 审计安全	
		实行远程办公的企业应定期对办公系统进行安全审计，审计内容包括但不限于对敏感数据的操作、访问控制权限变更等。

除上述管理和技术要求，实行远程办公的企业还应当特别注意员工等用户在设备、数据、环境方面注意以下问题，提高安全意识：

设备安全	a）应确保用户自有设备安装了正版软件、安全防护软件，并及时更新； b）应确保用户自有设备采用了安全配置，例如，关闭共享文件、禁用不使用的账号等； c）应对下载的文件进行病毒查杀； d）不应使用公用设备进行远程办公； e）宜将用户自有设备在企业登记。
数据安全	企业员工等用户 a）应采用企业（如雇主）指定的工具传输、存储、处理数据； b）宜减少从远程办公系统下载文件。
环境安全	在居家环境，用户 a）应使用路由器厂商提供的固件，并及时更新固件版本； b）宜在路由器中开启局域网防护等安全功能。 在公共场所，用户： c）在环境无法满足远程办公安全性要求时，应停止远程办公； d）不应在公共场所离开设备； e）不应使用不安全的网络，例如，无口令或公开口令的无线网络； f）宜防止设备屏幕被窥视，例如，使用防窥屏。
安全意识	用户： a）应使用强口令，并定期更新； b）应防范人员身份仿冒带来的风险； c）应使用办公邮箱，避免使用个人邮箱； d）不使用远程办公系统时，应及时退出； e）不应访问来源不明的链接、文档等； f）不应将存储使用方敏感数据的设备接入公用网络； g）不应将设备、账号信息等提供给他人使用； h）宜使用办公系统使用方提供的移动存储设备。

Your Contacts

ZHANG Yuhua
LL.M. (Nanjing & Göttingen)

Associate

Commercial & Distribution Law
E-Commerce
Cyber Security & Data Protection

+86 21 5010 7526
zhangyuhua@cn.luther-lawfirm.com

Languages: German, English, Chinese

Philip Lazare

Attorney-at-law (Germany), Partner

Corporate / M&A
Tax Law

+86 21 5010 6585
philip.lazare@cn.luther-lawfirm.com

Languages: German, English