君合专题研究报告

2020 年 3 月 30 日

疫情相关的信息保护和网络问题研究系列之二

——常态采用远程办公的注意事项讨论

前言

时至今日，疫情发展超乎最早的想象。下一阶段将会迎来返程复工的高潮。目前我们也注意到为了保证疫情控制和市民的安全，不同的机构和途径，都会采用各种方式收集个人信息并进行处理和分析。在这个过程之中，对于如何能够合法合规的收集信息、最小程度的影响被收集的信息主体的权利，并且能够有效地实现疫情防控是一个非常大的挑战，也是在以往的信息收集和处理的法律问题上没有遇到的艰难的课题。另一方面，企业在积极防范疫情的过程之中，如何应对远程办公所带来的网络和信息保护的挑战，也是另外一个相关的问题。

本篇研究之中，我们希望通过对于远程办公的全面采用进行一些分析，为企业在采用多种办公途径和选择的过程之中提供一些参考。

远程办公并不是一个新话题。此前很多公司已在探讨和实施各种灵活办公的方式，以给予员工更多的自由和选择，但仍然相对“小众”、“前卫”。疫情期间，为积极配合防控工作的开展，很多公司都采用了远程办公的方式。远程办公方式虽然便利，但实施的安全性、员工的隐私平衡、及同时提高办公效率，都是公司需要考虑、并逐步完善的。

一、员工使用第三方服务

员工在远程办公的过程中经常需要使用第三方提供的远程办公服务，例如在线会议、即时通信、文档协作等。一方面，第三方服务为员工进行远程办公提供了可能性和便捷性，但另一方面，也给企业带来数据安全、系统安全等潜在的风险。建议企业考虑以下几方面问题。

1、 区分网络安全责任主体

企业在让员工使用第三方提供的服务之前，应明确与该服务相关的网络安全责任主体。若企业所采购的第三方服务是部署在企业自身的服务器上，所属系统由企业自主管理，则企业应是该服务的网络安全责任主体；若第三方服务是部署在供应商的服务器上，企业对其所属系统并无管理权限，则供应商构成网络安全责任主体。

2、 审核第三方服务资质

企业在选择第三方服务时，应对第三方服务提供商的资质进行审核，是否符合基本的安全与技术要求，若服务或产品涉及到国家标准的强制性要求的，应审核是否已取得相关资质。根据全国信息安全标准化技术委员会于 2020 年 3 月 13 日发布的《网络安全标准实践指南-远程办公安全防护》的要求，企业作为使用方应充分评估第三方服务供应方的安全能力，包括但不限于安全开发运维、数据保护、个人信息保护等，并充分评估远程办公系统的安全性。

同时，考虑到中国法律对于数据出境的相关限制以及可能出台的进一步细则文件，如企业选择的第三方服务器部署在境外的，企业应当特别注意，并考虑出境的数据是否可以合法出境，并留存相关

记录。

3、 确保员工个人信息安全

员工在使用第三方服务时，第三方服务提供商很可能会收集员工的个人信息。一方面，在收集员工的个人信息前，企业或第三方服务供应商应通过隐私政策、知情同意书等方式向员工征求收集个人信息的同意；另一方面，企业应与第三方服务提供商签订数据安全处理协议等条款，确保第三方服务提供商对员工个人信息的存储和处理符合法律法规的要求。

4、 确保系统符合安全技术要求

参考《网络安全标准实践指南-远程办公安全防护》的规定，企业在使用远程办公系统前，应确保系统符合基本的安全技术要求，包括系统是否符合网络等保、云服务、个人信息保护等方面的安全要求，以及针对不同办公功能的系统的特定安全要求。除此之外，企业还应确保系统符合包括应用程序和浏览器在内的客户端安全要求。

5、 签署保密协议

员工使用第三方服务，可能存在将涉及企业商业机密的信息上传至第三方的情况，在这种情况下，企业应与第三方服务提供商签署保密协议。防止商业机密和其他重要数据的泄露。

二、员工使用自有设备

对于企业而言，允许员工使用自有设备能够减少企业在设备方面的开支，有利于员工更迅速的响应工作要求。但是，员工使用自有设备，也会带来一系列相应的数据安全和个人隐私问题。特别是允许员工使用自有设备可能构成对企业网络与数据安全的威胁。出于远程工作的需要，员工可能通过自有设备连接企业的内网或访问企业的内部系统。若企业无法对员工的个人设备进行安全监控与管理，而员工在其设备上无意间安装了设置有恶意程序的插件，或点击了带有病毒的邮件或钓鱼邮件，企业内部网络的安全将受到被攻击的威胁；此外，员工使用自有设备进行工作，可能会将企业的内部机密信息存储在终端设备中，一旦终端设备丢失或被恶意地破解，企业的信息面临被窃取、丢失的可能性。另外，在发生需调查员工相关合规事件时，企业也存在合法取证的困难。企业可考虑以下方面措施。

1、 制定自有设备安全使用制度

企业可制定内部的自有设备安全使用制度，并对员工进行相关培训，提升员工的安全意识。

2、 建立访问权限制度和数据分级管理制度

基于员工使用自有设备访问企业内部系统，造成的系统安全和数据泄露的风险较大，企业可对员工使用自有设备访问企业内部系统的访问权限进行限制，并建立数据分级管理制度，对于机密性较高的数据，限制员工通过自有设备访问或获取。

3、 制定网络应急预案

针对使用自有设备可能发生的网络安全事件，企业应制定网络安全应急预案，完善网络安全事件报告机制，及时对网络安全事件做出应对。

三、采取适当监控措施

在远程工作的过程中，企业出于对员工进行管理和监督的需要，可能会采取对员工进行远程监控的措施。例如，企业可能通过摄像头监控员工的工作状态，或者通过插件追踪员工的网络浏览记录。一般情况下，为了实现远程监控的目的，企业不可避免地会收集员工的个人信息，因此，如何平衡对员工的远程管理与保护员工隐私之间的关系，是远程工作中企业需要重点关注的议题。

实践中，企业应谨慎考虑是否通对员工进行远程监控的方式。由于《网络安全法》等相关法律法规要求收集使用个人信息要符合合法、正当、必要的原则，因此，若企业计划在远程工作中通过实施监控，例如通过摄像头、或其他网络技术手段进行监控，首先需要考虑收集的数据和收集的目的是直接关联的、并且符合比例原则。如企业经过评估，认为使用该种方式确有必要的前提下：

- 企业可通过知情同意书等形式向员工告知为了采取监控措施所需要收集的个人信息的类型和方式，并获得员工的明示同意。

- 不得将员工的数据用于工作监测以外的目的。
- 采取必要措施确保信息在传输和存储过程中的安全。
- 仅在工作时间内开展监控。

四、我们的观察

疫情期间为远程办公的实现提供了大规模的试验期。一方面，为远程办公的相关服务会快速增加和迅猛发展，为企业员工提供更便利的工作渠道。另一方面，由于远程办公带来的信息安全风险、隐私权利的争论也会不可避免的增多。企业只有早做部署，全面、提早考虑各种渠道，通过法律、技术等各方面的机制来保证企业自身的信息安全、权利平衡和实施的合规性，才能将远程办公的便利性发挥到极致，也将推动未来更深入的工作方式变革。

我们愿意持续与不同企业探讨这些新的方式和挑战，并为这些新问题提供相应的解决方案和建议。

董　潇　合伙人　电话：86 010 8519 1718　邮箱地址：dongx@junhe.com
袁　琼　律　师　电话：86 010 8553 7663　邮箱地址：yuanq@junhe.com
董俊杰　律　师　电话：86 010 8540 8722　邮箱地址：dongjj@junhe.com