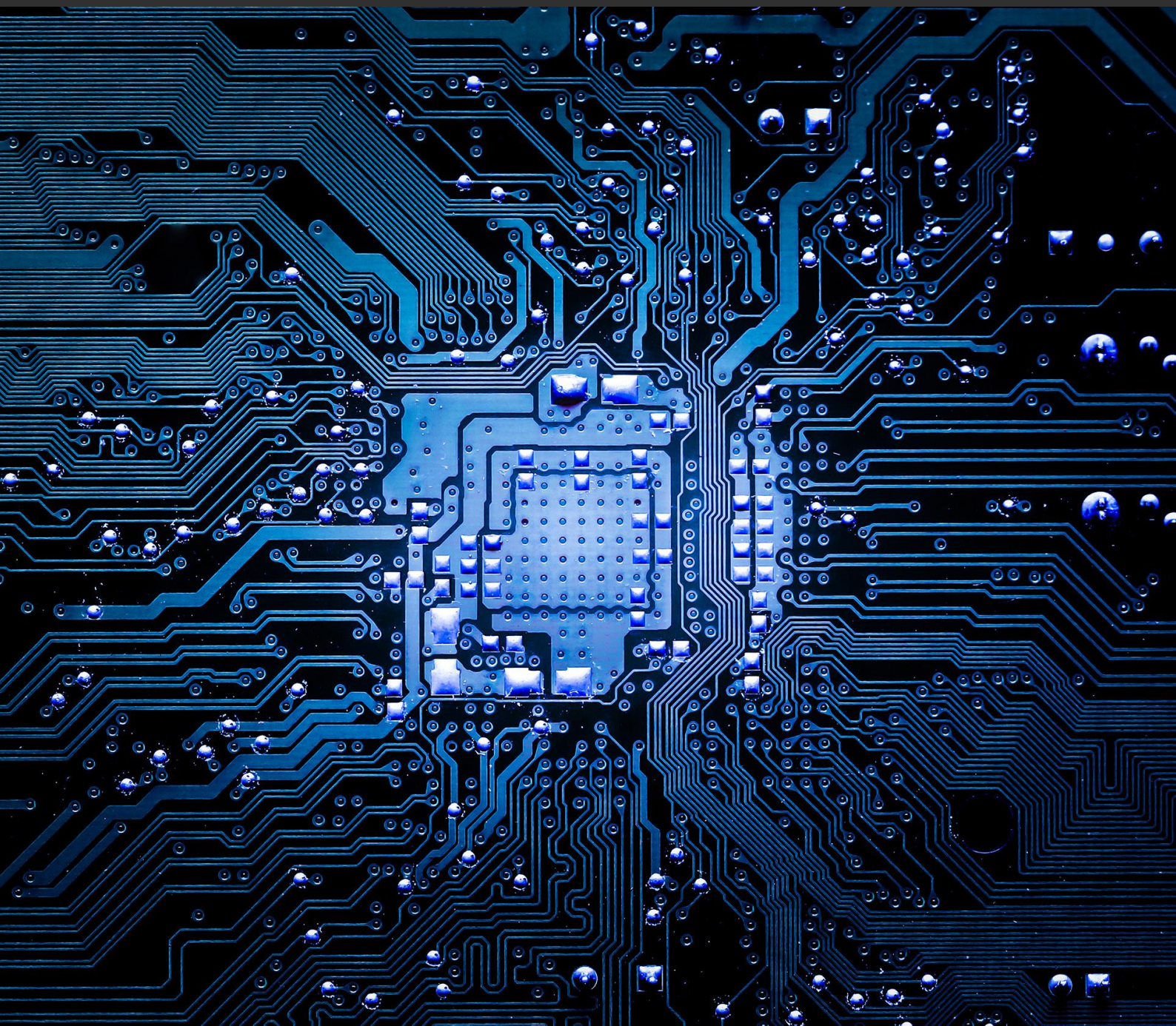
simmons+simmons

Impact of EU AI Act on Chinese companies

English summary and Chinese transcript

2025

STRICTLY PRIVATE AND CONFIDENTIAL



This is a summary from an online seminar discussing the European Union's Artificial Intelligence (AI) Act, which became effective on August 1, 2024, and its impact on Chinese companies. It is the world's first comprehensive law targeting AI, imposing clear legal obligations on AI developers and users. The seminar highlights several key aspects of the AI Act:

1. **Risk-Based Approach:** The AI Act categorises AI systems based on risk levels, applying different requirements for each category.
2. **Applicability:** The law applies to both AI developers and users, including tech companies and their clients, like banks using AI systems for resume screening.
3. **EU-Wide Application:** The AI Act uniformly applies across EU member states without needing transposition into national laws.
4. **Penalties:** Violations can lead to substantial fines, up to €35 million or 7% of the global turnover for the most severe breaches.
5. **Implementation Timeline:** The Act's provisions will be fully implemented by August 2, 2026. However, certain parts, like prohibitions on high-risk AI systems, will come into effect earlier.
6. **Extraterritorial Effect:** The AI Act also affects non-EU companies providing AI systems in the EU or affecting individuals within the EU.

The seminar also delves into specific obligations for high-risk AI systems, including risk management, data governance, transparency, and cybersecurity measures. It emphasizes the importance of AI literacy for employees and stakeholders involved with AI systems.

For companies, especially those outside the EU, it's crucial to analyse the impact of the AI Act on their operations and ensure compliance with its provisions. The seminar encourages companies to stay informed about upcoming guidelines and standards to navigate their compliance journey effectively.

Learn more about our Artificial Intelligence expertise at this link and view the rest of the webinars in this series here. A Chinese transcript follows.

Jingyuan Shi
Partner and Head of TMT, Greater China
T +852 2583 8346 (Hong Kong)
E jingyuan.shi@simmons-simmons.com

Jenny Liu
Managing Associate
T +86 755 3368 9398
E jenny.liu@simmons-simmons.com

Yuchen Lai
Supervising Associate
T +86 755 3368 9397
E yuchen.lai@simmons-simmons.com

Jingyuan Shi

大家好，我是西盟斯中国办公室合伙人史晶源，也是我们中国区TMT法律业务的负责人。

今天我和我们深圳办公室的两位核心成员 Jenny （刘姝琪）和 Yuchen （赖雨晨）会和大家一起探讨《欧盟人工智能法》对于中国企业的潜在影响。这次的探讨是我们西盟斯关于《欧盟人工智能法》，也叫 EU AI Act，这个系列在线讲座的其中一场，也欢迎大家访问我们的官方网站 (Simmons & Simmons.com)，浏览、收看更多的相关内容。

这部法案是在2024年8月1日正式生效的，也是全球第一部针对 AI 的综合性法律，对 AI 的开发者和使用者提出了明确的法律义务和要求。有这样几个特点，想和大家先分享一下。

第一个特点就是这部法案采用了着眼于风险的方法，按照风险来分类，对不同的 AI 系统和 AI 模型提出了不同的要求。

第二个特点是它既适用于 AI 系统的开发者/提供者，也适用于 AI 系统的使用者/部署者。比如说我们一家科技公司开发了用于筛选简历的 AI 系统，那么另外一家银行采购并使用了这套系统，不管是这个科技公司还是这家银行，他们都可能受到 EU AI Act 的约束。当然，约束程度根据他们不同的角色有可能是不同的。简而言之，就是开发者/提供者所受到的约束，要比使用者/部署者要严格。

第三个特点是这部法案统一适用于欧盟成员国，不需要经过国内法的转化适用，它是一部覆盖欧盟成员国的、可以直接适用的欧盟法。

第四个特点是处罚高昂。针对违反的相关法律规定的不同，看是违反的是哪条规定，分为几个等级。如果违反的是被禁止的规定，那么可能导致高达3500万欧元或者相关集团上一年度全球营业额7%的处罚。如果违反的是其他条款，可能导致最高额达1500万欧元或者上一度多全球营业额3%的罚款，差不多比一半还少一点。那么如果是向监管机构提交不准确不完整或者误导性的信息，那罚金就再打折，就可能导致750万欧元或者上一年度全球营业额1%的罚款。

生效时间方面，法案的规定是将在生效后两年，也就是在2026年的8月2日全面实施。在此之前，欧盟将陆续的出台相关的标准指引、行为守则等文件来指导企业实现这部法案项下的义务合规。

但是需要注意的是，这部法案的部分条款有特殊的实施时间，包括以下几种。第一种是针对禁止性规定，也就是那些针对带有不可接受风险的AI系统的禁止性规定，还有和 AI 素养相关的规定，将在法律生效后6个月也就是2025年2月2日首先实施。第二个点是针对通用目的 AI 也叫做 GPAI 的规定，将在法律生效后一年也就是2025年的8月份实施。最后一个实施的时间级别是针对一部分的高风险 AI 系统，也就是这部法案附件I所列的这些高风险的 AI 系统，将在法律生效后3年也就是2027年的8月2日实施。那么这也意味着基于受到约束的具体产品，AI 系统、AI模型的不同，企业需要合理安排采取合规行动的时间。

Jingyuan Shi

最后一个想说的点是这部法案规定了非常广泛的域外效力，影响力会超过欧盟的范围。比如说如果中国企业面向欧盟市场提供或者许可 AI 系统，又或者是中国企业使用AI系统对欧盟境内的人群产生了影响，都有可能落入这部法案的管辖范围。

因此，我们建议中国企业采取分步骤分析的方式，识别这部法案对于自身的影响，从而更好地开展下一步的合规工作。接下来就请我的同事Jenny和雨晨从这部法案的约束对象、企业角色、域外效力和风险分级这四个角度跟大家详细讲解一下，什么是分步骤分析的方法。

Jenny Liu

谢谢晶源。接下来在我们这一部分，会展开来讲我们作为一个中国企业，如何判断这部《欧盟人工智能法》是否适用于我们企业，以及在多大程度、多大范围内会适用到我们企业。

第一个我们需要解决的问题，就是这部《欧盟人工智能法》它所约束的主要的对象是人工智能系统，那么什么叫做人工系统呢？法律当中对于人工智能系统的定义是指基于机器的一个系统，而且这个系统在不同程度上可以去实现自主运行，并且可以表现出一定的适应性，也就是说它可以针对它所接收到的输入物来去推断、推导出来，并且生成输出物，这样的一个系统我们把它叫做人工智能系统。我们列出来了几对概念，是我们认为在判断这个系统到底是否人工智能系统时候需要着重去看的几个定义。

第一个就是人工智能和自动化的区别，首先一个自动化的系统，它其实也可以实现，比如说在不同程度上去进行自主的运行，那么对于一个自动化系统和人工智能系统之间的主要的区别，其实就是在于这个系统到底有没有这样一种能力，它可以从它接收到的输入物中推断、推导得出一个输出物。如果具备这样子推断的能力，那我们就把它认定为是一种人工智能。

第二对概念就是有关于什么是人工智能系统，以及什么是人工智能模型的区别。简单来说，人工智能系统其实是一个更加完整的产品。比如说绝大多数最终用户它所接触到的其实都是人工智能的系统或者人工智能的一款应用。这个系统就包括用户的交互界面，也包括它去接收输入物和导出输出物的这两个接口。而如果我们说的是一个人工智能模型的话，往往指的是比如说大语言模型，这个模型这个算法本身。所以《欧盟人工智能法》其实主要的监管对象在于前者，就是人工智能系统。另外补充一个背景，其实在《欧盟人工智能法》的前几稿当中，它的监管对象都只限于人工智能系统，但是在最后定稿的时候，它加入了第五章这个章节，反而把约束对象延伸到了某些类型的人工智能模型，所以我们待会儿可以再详细看一下法案对于人工智能系统和人工智能模型都相应提出了怎样的法律义务。

最后一对我们需要去详细了解的概念，就是通用目的的人工智能模型和具有系统性风险的人工智能模型。通用目的的人工智能模型是指在使用大量数据去进行自我训练的时候，这个模型它显示出了一定的通用性，也就是它可以去胜任不同的具体的任务，并且它可以方便地去集成到各类下游的人工智能系统或者人工智能应用当中。如果它表现出这样的通用性，那么我们就把它称之为一个通用目的人工智能。通常来讲我们所了解到的，比如说 OPEN AI 的 GPT，比如说百度的文心一言，包括我们很多其他国产厂家的，比如腾讯的一些混元大模型，阿里的通义千问等等，这些其实都会被认定为通用目的的人工智能模型。

另外一类就是具有系统性风险的通用目的人工智能，这一类模型基本上法律认为它是在当今世界当中最先进的一类的人工智能模型，它具有比较高的影响力。如何去判断一个人工智能模型，它到底具不具有这种高影响力，是否具有系统性风险呢？一个直观的判断因素就是在训练这个模型的时候所用到的累计计算能力，是否达到了我们这里写的10的25次方的这个标准。如果达到这样的标准，我们就把它推定为是具有高影响力的，也就是具有系统性风险的一个通用目的人工智能模型。相应的，具有这类系统性风险的通用目的人工智能模型，法案就对它的开发者、提供者，去提出了更高的、更严格的法律要求。

Jenny Liu

接下来我们想看的一个问题就是，如果确实企业在不同的环节当中用到了这个人工智能系统，那么它相应承担什么样的法律义务，是由这个企业在人工智能产业链当中，它到底处于什么样的一个地位，处于什么样的角色来决定的。我们列出了人工智能法当中提出的最主要的四种角色：提供者、进口商、经销商和部署者。其中提供者和部署者又是这个法案当中着重强调，并且相对来讲义务更重的两个角色。

作为提供者，简而言之，其实就是人工智能系统的开发者。它既包括投放到欧盟市场或者在欧盟提供服务的人工智能系统的开发者，也包括以企业自身的名义去投放到欧盟市场上的通用目的人工智能模型的开发者。比如说，对于 GPT 而言，那么就是指的 OPEN AI，但是并不包含其他调用了 GPT 作为它基础模型的其他的人工智能系统的开发者。这是第一个有关于提供者的角色。

第二个我们想着重去看的就是有关于部署者，部署者其实简而言之就是人工智能系统的使用者，对人工智能系统的使用行为去承担最终责任的这个人。但是法律其实排除掉了以下情形，企业在这种情形之下，它其实不视为是部署者——比如说，如果我是一个自然人用户，我把这个人工智能系统用于完全的个人目的，或者非专业性的活动当中。比如说我作为一个普通公众，我出于自身娱乐的目的而使用了一个通用目的人工智能系统或者系统的模型，那么这个个人用户并不会因此而被认定为《欧盟人工智能法》下的部署者，并且需要去遵守这部法案项下对于部署者施加的相应的法律的义务。

然后另一个点，我们想强调的就是这部法律当中，对于提供者和部署者其实都不限于它是欧盟境内还是位于欧盟境外的。我们待会儿也会详细地讲到在什么样的情形之下，一个位于欧盟境外的提供者有可能就会落入这部法律的管辖的范围。

接下来我们再来看一下有关于进口商和经销商的两个角色。进口商简而言之，就是指将欧盟外的公司的人工智能系统投放到欧盟境内，使这个系统第一次进入欧盟市场的这个人，我们叫做进口商。经销商就是指在欧盟市场上去提供这一项人工智能系统的，但是它本身又并不作为提供者，它可能只是一个转售商的角色。

这里我们需要强调的就是一个公司，它有可能同时担任经销商和进口商的角色，也就是它有可能既是第一次把这个系统引入到欧盟境内的，同时它也是继续在这个欧盟市场上进行销售的这个人。那在这种情况下，它就是同时担任了进口商和经销商的角色。相比较而言，进口商和经销商两个角色在欧盟人工智能法下承担的法定义务是相对较轻的，所以我们在下一个章节当中也会详细地展开有关于提供者和部署者的法律的义务。

最后我们想要说的是，一家企业它到底是一个人工智能系统的提供者还是部署者，其实并不是一成不变的。可能对于A系统而言，它属于一个使用者的角色，它就属于部署者，但是对于B系统而言，它又是直接去开发这个系统的，那它对于B而言就是一个提供者的角色。那同时对于这个高风险的人工智能系统来讲，在特定情况下，一个部署者也有可能被法律认定为一个提供者的角色，并且因此而承担上对于提供者的一些法定的义务。

Jenny Liu

比如说我们这边说到的第一种情形，如果这个系统是一个现有的，它是一个高风险的人工智能系统，而我在使用过程当中，我把这个系统打上了我自己企业的名称或者商标来去进行使用，那这种情况下，我这个企业其实不单单是一个单纯的使用者了，它有可能被法律认定为这个系统的提供者，因此而承担较严格的这个法律义务。

第二种情形就是现在有一个现成的高风险的人工智能系统，那我在使用它的时候，我对于这个系统去进行了一些实质性的修改，然后修改之后这个系统仍然会被法律认为是一个高风险的人工智能系统，那么我做出这个实质性修改的这个人，其实也有可能被法律认定为一个提供者。

第三种情形就是针对一个它原本其实并不是高风险的，它是一个普通的人工智能系统，但是我去进行了一些改变，比如说我改变了它的用途，把它用在更加敏感、更加高风险的一些场景之下，使之就成为了或者符合了法律项下对于高风险 AI 的定义。所以在这种情况下，我后面的这个改变用途的企业，也会被法律认定为一个提供者的角色。

出现这种情形它直接的影响和法律上的后果是什么呢？第一个对于原本的这个系统的开发者而言，它就不再成为法律项下的这个提供者，而是由实施了这些改变或者改变用途的后面的这个企业来去视为新的这个系统的提供者。第二点就是原来的这个开发者，法定项下它有义务向新的提供者去提供一些有关于这个系统本身的一些信息和技术，以辅助这个新的提供者来去完成它作为提供者在法律项下的一些义务。当然这个我们说的是法律层面对于两者的角色定位和义务的划分，其实在合同层面很有可能各方当事人之间也对于法定义务的具体的承担和具体责任义务的履行方式等等，做出一系列的合同层面的约定。

接下来我们想强调的一个重点的问题就是我作为一家中国公司，在什么样的情形下，我需要去考虑这个《欧盟人工智能法》，在什么样的情形下我会落入它的管辖范围。

这边我们罗列出来了主要的四种情形，其实第一种情形我们并不把它称之为《欧盟人工智能法》的一个域外效力，它其实仍然是域内效力的一个表现形式。假设说我是一个中国总部的公司，但是我在荷兰建立了我的子公司，那这个荷兰子公司在欧盟境内，比如在荷兰去使用一些人工智能系统，在它的日常经营活动当中，这种情况下，其实这个荷兰子公司在欧盟境内的这种使用行为，它是会被落入到《欧盟人工智能法》。这点其实不难理解，就是比较正常的域内效率的这个适用范围。

第二种情形，我们这边列出的就是如果是向欧盟市场去销售或者去许可一个人工智能系统或者通用目的的人工智能模型，即使我这个销售或者许可的提供者，它是位于欧盟境外的，那也有可能会落入到《欧盟人工智能法》的这个管辖范围内。比如说我们这边提到的两个例子，我是一家中国公司，然后我向我的客户一家法国公司去销售我中国公司自主研发的这个人工智能系统，那么我会被认定为这个人工智能系统的提供者，而因而需要去履行《欧盟人工智能法》下对于提供者的一些法定义务。第二种情形就是，如果我作为一家中国公司去向我的客户法国公司去许可了我自己开发的一个人工智能模型，而这个法国公司利用我的这个人工智能模型继续地集成，并且开发出来了他自己的人工智能的应用或者人工智能的系统。那么我作为一个中国公司，我其实仍然会被认定为这个提供者的角色，因此需要符合《欧盟人工智能法》下对作为提供者的一个法定的义务。

Jenny Liu

第三种情形就是，我作为人工智能系统的提供者或者我作为它的部署者也就是它的使用方，我是位于欧盟境外的，但是这个系统产生的输出物是用于欧盟境内的。那什么叫做这个输出物是用于欧盟境内的呢？我们现在的理解，其实它往往指的就是一种情况，比如说我把这个人工智能系统去用于分析欧盟境内个人的一些行为模式，或者我利用这个人工智能系统的输出物对于欧盟境内的一些个人去产生了一些影响，比如说我因此做出了一些是否招聘他的决策，是否去给他做一些定制化的营销等等决策。在这种情况下，我们就会认为这个系统的输出物是用于了欧盟境内。这边我们举到的一个例子，也就是我作为一家中国公司使用了人工智能的系统去分析位于欧盟境内的用户，比如说我去分析他的一些使用行为，去分析他的对于产品的一些偏好等等，或者说我去分析我在欧盟境内其它子公司的一些员工的情况，去评估它的工作的效率，评估它的报酬机制等等，这些也都叫做把输出物用于欧盟境内。

最后一种情况就是我作为一个产品的制造商，我的产品当中是集成有人工智能系统的，那我作为制造商把这个产品投放到欧盟市场上的时候，我其实作为产品制造商的角色，我也会受到这个《欧盟人工智能法》的约束。比如我们这边举到的一个例子就是我是一家中国的手机制造商，我向欧盟去销售一款手机。这个手机本身是带有一个人工智能系统的，而且这个人工智能系统以及这个手机产品本身都使用到了我中国企业的名称或者品牌，是以我的名义去卖到市场上去的，那这种情况下，其实我在欧盟境内去销售这种带有人工智能系统的产品，那就会落入到《欧盟人工智能法》的这个监管范围之内。

接下来我们想讲一下，如果我作为一个中国公司，我在欧盟境内既没有子公司，也没有相应的人员，那我如何去履行《欧盟人工智能法》对于我施加的一些义务，尤其是我如何去向欧盟的监管机关去做一些报告、去做一些登记注册等等。

这个时候，《欧盟人工智能法》就要求中国公司在欧盟境内去指定一个授权代表。这个授权代表，首先他所适用到的范围，如果你是向欧盟市场上去提供人工智能系统或者通用目的人工智能模型的提供者，才需要去指定欧盟境内的授权代表，这是第一点。

第二点，关于这个授权代表，他需要符合什么样的条件呢？第一个就是这个授权代表既可以是一个个人，也可以是一个法人来担任，但是他必须是一个位于欧盟境内的个人或者是法人，并且他做这个授权代表必须是基于中国企业，作为这个人工智能系统的提供者，给到他的一个书面的授权。这个书面的授权当中需要去比较详细地去列举出来，这个授权代表他的职责范围是什么，以及他所授权的权利范围是什么。

接下来我们再详细看一下，作为一个欧盟境内的授权代表，在《欧盟人工智能法》项下具体的职责是哪些？比如说第一项他需要去检查、去确认这个中国企业作为提供者，它是否已经起草了法案要求的欧盟一致性声明，以及相关的系统技术文件，是否已经建立了企业内部有关欧盟一致性评估的内部程序。

第二点就是关于文档的保存和信息的保存管理，也就是作为授权代表，我需要去保留中国企业的这个联系方式，它的一致性声明、技术文件以及给到欧盟境内通知机关的所发布的一些证书等等，并且这个保存期限需要达到十年。

Jenny Liu

第三点其实是针对于高风险的人工智能系统，以及通用目的的人工智能模型而言。如果我接收到了监管机关的一些要求，那么这个情况下，授权代表需要向监管机关提交一些必要的信息和文件来证明这个系统是符合《欧盟人工智能法》的。

第四点就是有关于配合监管机关去采取一些行动，来减轻有关于高风险人工智能系统的风险。

第五点就是如果这部法案要求到人工智能的系统或者是人工智能的模型去完成一些登记注册的话，那么这个授权代表需要去协助完成这些登记注册的手续。

最后我们想要强调的就是，虽然这个授权代表是基于中国企业对于他的一个书面授权，但是实际上这个授权代表他是有一定的独立性的。比如说他如果在工作当中一旦发现了，或者它有理由认为这个中国企业作为人工智能系统的提供者存在违法的情况，那么这个时候授权代表需要立即地终止授权，并且还需要去通知相关的监管机关以及说明理由，为什么我现在不能担任这个授权代表的角色了，我是发现了哪些违法的行为，所以这个时候需要注意一下，授权代表他其实相对于企业来讲的话，还是有一定的独立以及监督的职能。

接下来就由我的同事雨晨来跟大家详细地讲述一下人工智能法项下对于不同等级、不同类型的人工智能系统去施加了哪些具体的合规义务。

Yuchen Lai

好的，谢谢 Jenny。刚才通过 Jenny 的介绍，我们知道结合这个产品具体的人工智能系统或者是模型，结合企业的角色和地域，企业已经可以初判断自身是否受到《欧盟人工智能法》的管辖。接下来，大家还需要进一步地去分析，每一个人工智能系统和通用目的人工智能模型的风险分类。因为不同的系统和模型，它们可能面临不同的合规义务，而且相关规则的实施时间也是各不相同的，只有对这些风险的分类了然于胸，我们才能够从容、合理的去规划相应的合规行动。

首先我们来看一下有哪些类型的 AI 的实践是有不可接受的风险，因此被《欧盟人工智能法》所禁止。这里所说的不可接受的风险主要是指会侵犯欧盟《基本权利宪章》所规定的一些基本的权利，包括几大类型。比如说利用人的弱点，利用操纵和使用潜意识技术；比如说使用 AI 去根据社交行为或者是个性特征对人进行评估和分类，我们也叫做社交评分；比如说利用 AI 去对互联网或者是闭路电视 CCTV 去进行一种非定向的数据爬取，来创建或者扩展面部识别的数据库；还有在工作场所或者是教育环境中，根据生物识别数据，来推断情绪的这种人工智能的使用（当然，在这个中间有一定的例外，比如说如果是为了医疗或者是安全目的的使用，例如我们去监测一个飞行员的疲劳程度，那么这种它就不属于是一个不可接受的风险，因为还是有一定的合理性的）；再比如说，根据一些敏感的特征，利用生物识别数据对个人进行分类；以及为了执法的目的在公共场所使用人工智能进行实时远程的生物识别等等。

这一类被禁止的 AI 实践或者说不可接受的风险，相对的范围还是比较有限的。但是我们想提醒大家注意的就是，相关的规则是在2025年2月2日就会实施了。在这个期限之前，欧盟委员会会出台一个专门的指引，而且在2024年的11月13日到12月11日之间，欧盟委员会已经向相关的 AI 系统的提供者，还有成员国的监管机构以及学术界和社会团体等等的利益相关方定向征求意见。预计出台的指引也会包含一些各界反馈的实例，如果企业的 AI 系统有可能涉及到刚才我们所列举的这些应用场景的话，需要密切关注欧盟委员会即将出台的指引，因为如果违反了相关的规定，相应的处罚是非常严厉的。

接下来我们再来看一下所谓的高风险的 AI 系统，这里面主要包括两类情形。第一类的情形，我们可以简单的把它概括为高风险的产品。它指的是人工智能系统是受到特定的欧盟法规所约束的产品，或者是产品中的安全部件，而且根据欧盟法律要求，是需要通过第三方的合规性评估的。那么这里所说的特定的欧盟法规指的就是人工智能法附件I所列出来的欧盟法规，包括针对机械、玩具安全、电梯、医疗器械、航空等等的一批的欧盟的指令和条例。

例如说，如果一个人工智能系统被作为安全部件集成到了医疗器械、玩具、车辆里面，那么它就很有可能被视为一个高风险的人工智能系统。或者说，如果这类产品本身就是一个人工智能系统，例如说我们看一个玩具，如果它实质上就是一个人工智能的一个声控助手的话，那么它也很有可能被视为是一个高风险的人工智能系统。

第二类情形，我们可以把它概括为是一种高风险的应用场景，也就是《欧盟人工智能法》附件III所列的人工智能系统，涉及到远程的生物识别、情绪识别、关键基础设施的运营管理、招聘、人力资源管理、选举等等的不同的场景。

Yuchen Lai

我们想特别提醒大家留意的，是关于这个招聘和劳动关系管理的场景。因为这个场景可能在不同行业的跨国公司，包括很多总部在中国的公司，很有可能是大家所广泛使用的。例如我们通过人工智能的决策的推荐，去做出一些可能会影响劳动关系的一些决定，影响员工的晋升，影响终止劳动合同的决策，包括可能会有一些基于个人的行为、特质、性格，去给他们分配工作任务等等。那么这些，其实都是属于高风险的应用场景。除了这一些场景之外，未来欧盟委员会还可能继续补充或者调整附件III的范围。

针对高风险的人工智能系统，提供者承担了比较繁重的义务。这里面我们可能就挑选其中的一些，因为时间关系，重点跟大家说一下。例如，实施风险管理的系统，指的是在高风险人工智能系统的整一个生命周期里面，我们需要去规划和运行一个持续迭代的过程，去定期进行系统的审查和更新，包括要能够按照预期的目的去识别和分析高风险人工智能系统对于健康、安全或者基本权利造成的已知的、以及可以合理预见的风险，还要去估计和评估高风险人工智能系统可以预见的误用的风险，以及根据上市后监测收集到的数据评估其他的风险，以及对风险采取适当的管理措施。

再举一个例子，像是数据治理，指的是使用数据训练、验证和测试高风险的人工智能系统的时候，都必须要遵循特定的质量标准。例如用于训练、验证和测试的数据集，必须是具有相关性的，而且要有完整性和充分的代表性，而且是能够尽量的去减少错误。

我们再来看一下透明度的要求。高风险人工智能系统的设计和开发，需要确保它的运行是具有足够的透明度。什么样叫做足够的透明度呢？就是要使下游的部署者能够解读到系统的输出物，并且去适当地使用，而向下游部署者需要提供的信息要包括系统提供者的身份和联系方式、系统的特点、它的性能和局限、人工监督的措施，包括为了便于部署者解读系统的输出物而采取的技术措施所需要的计算和硬件资源、高风险人工智能系统的预期寿命，以及任何必要的维护保养措施等等。那么大家可以看到透明度的要求，需要提供的这些信息是非常全面的。

最后我们再来讲一下网络安全，高风险人工智能系统是需要有能力去抵御这种未经授权的第三方利用，从而防止第三方通过这种系统漏洞去改变它使用、输出或者性能。那么人工智能法还特别提到了几类针对人工智能特定漏洞的网络安全风险，而且明确要求对这一类的风险进行预防、检测、控制和应对。这些风险包括数据中毒，也就是试图篡改训练数据集，也包括模型中毒，例如试图去篡改训练中使用的这些预训练的组件，包括对抗性示例，或者模型规避、保密性攻击或者是模型缺陷等等。

针对高风险人工智能系统的部署者也有相应的合规义务。首先是需要按照提供者它们所提供的这个使用说明，来部署和使用高风险的人工智能系统，也就是说我们在使用的时候是必须遵循特定的一些规范，不能够随意地、任意地去使用。

第二个是对高风险的人工智能系统要实施人工监督，而且相关的监督人员必须要具备必要的能力，经过培训，而且有足够的权限和支持。

Yuchen Lai

第三点，是对系统的使用进行监控，如果我们发现按照规则使用系统可能会带来基本权利、健康或者安全方面的风险，就需要及时的通知系统的提供者。或者是经销商以及市场监管机构，并且要暂停使用这个系统。如果发现了严重的事故，部署者需要首先通知提供者，然后再通知进口商、经销商和市场监管机构。

第四点是针对高风险的应用场景，在做出和自然人有关的决定或者协助做出与自然人有关的决定的时候，应该是要告知自然人这里面是有使用到高风险的人工智能系统。

高风险人工智能系统相关规定的实施时间是在2026年的8月2日和2027年的8月2日，有两个阶段。在此之前，欧盟委员会也会出台进一步的指引。

接下来，我们看一下第三个风险层级，第一个是被禁止的，第二个是高风险的，第三个风险层级其实就是刚才 Jenny 也重点介绍的通用目的的人工智能模型以及具有系统性风险的通用目的人工智能模型。通用目的的人工智能模型是可以用作各种任务的，而且因为单个模型可以集成到大量的下游的人工智能系统中，所以它其实处于这个产业链的上游。下游的这些系统的提供者需要获得所有必要的信息，才能够确保系统的安全并且符合法律的规定。

因此，《欧盟人工智能法》就规定了通用目的人工智能模型的提供者有义务要向下游的系统提供者去披露特定的信息。此外，通用目的人工智能模型的提供者还需要制定相应的制度，确保在训练模型的时候遵守版权法。

具有系统性风险的通用目的人工智能模型就需要遵守更加严格的规定。现阶段，如果用于训练模型的累计计算能力达到或者超过10的25次方每秒浮点运算次数，就会被默认视为具有系统性风险。那么，根据斯坦福大学在2024年8月发布的一份报告截止到当时市场上至少是有8款的大语言模型已经达到了这个标准。其中也包括一款由中国企业开发的模型，那么我们考虑到国产大模型的快速发展，也相信会有更多的中国企业的模型触发到这个门槛。需要特别注意的是，系统性风险的这个门槛，它并不是固定不变的。欧盟委员会会根据技术的发展来更新计算能力的门槛，还可能依据其他的指标来指定其它的系统性风险。这些指标可能包括用户的数量和模型的自主性水平等。

对于具有系统性风险的通用目的人工智能模型，模型的提供者就需要履行一些额外的义务。第一个是需要根据反映最新技术水平的标准化协议和工具来进行模型的评估，包括对模型进行对抗测试，而且保存记录，用来识别和降低系统性的风险。第二点是需要评估和降低在欧盟层面可能因为开发、投放和使用具有系统性风险通用目的人工智能模型而导致的风险。第三点是要跟踪记录严重事故的信息以及采取纠正的措施，而且要向欧盟的人工智能办公室进行报告。第四点，是对模型和模型所依托的物理基础设施采取适当的网络安全措施。

我们还想特别提醒，由于这种通用目的人工智能模型它是处在人工智能系统开发的上游，因此针对模型的规定会在2025年的8月2日实施。也就是说比整个人工智能法的全面实施的时间是提早了整整一年的，因此相关的这些合规工作也需要优先安排。

Yuchen Lai

我们再看实际情况中的一些例子，如果一家中国企业，它是有开发大语言模型的能力，同时它也基于这个大语言模型推出了一个用在手机上的这种智能助手的 APP，那么这个 APP 它就会是一个人工智能的系统。针对这个模型和针对这个系统，同一家公司可能需要满足不同的合规要求，而且这些要求实施的时间点也不一样，因此就需要以不同的优先级去采取行动。

目前，欧盟的人工智能办公室正在制定有关于通用目的人工智能模型的行为守则，目的就是为企业提供具体的合规指引。在2024年的11月14日人工智能办公室发布了由独立专家起草的行为守则的初稿，而且计划在2025年的5月2日之前要发布定稿版本的行为守则。我们也建议相关的企业需要密切关注守则的初稿的内容，以及它后续的修改和发布。

除了刚才重点提到的被禁止的、高风险的人工智能系统，以及通用目的人工智能模型之外，其他的人工智能系统主要面临的是透明度方面的义务，具体要求会因为系统的类型和使用场景而有所不同。这部分要求将在2026年的8月2日起正式实施。同样的，欧盟委员会也会在此之前出台相关的指引。

接下来，我就把时间交回给 晶源，请她来为我们总结一下目前企业所面临的最紧迫需要完成的一些准备工作。

Jingyuan Shi

好的，谢谢雨晨。正如我们在这一次讨论最开始所谈到的，这项法案项下的规则将在明年2025年的2月、8月，2026年的8月，2027年的8月分阶段实施。因此留给企业的准备时间会因为我们讨论的具体产品的不同而有差异。

我们因此建议企业尽快分析这部法案对于贵司自身的相关系统的适用情况，制定相应的合规时间表。如果我们看最早一批实施的规则，会包含两个比较重要的方面。第一个是最早于2025年2月份开始实施的规则。一个是适用于具有不可接受风险的 AI 系统的这些禁止性的规定。这部分的违规会面临极高的处罚，如果企业的产品确实可能触及这一门槛的话，需要密切留意欧委会即将出台的指引，指引刚刚在2024年12月11日结束征求意见。

另外一个重要的方面是有关AI素养的义务，也就是 AI Literacy。法案规定，AI 系统的提供者和部署者需要确保员工和其他相关人员具有足够的 AI 素养。什么是 AI 素养、具体包含哪些要求，又是一个相当复杂的话题。但这是一项普遍适用的义务，也是最先实施的这个义务之一，我们也已经开始为我们的一些客户开发了面向内部员工的 AI 素养课程。如果您对这个话题感兴趣，也欢迎来和我们进一步的探讨。

以上就是今天我们希望和大家分享的内容。再次重申，这次讲座是我们关于欧盟人工智能法案系列在线讲座的其中一场。如果大家对这个话题感兴趣，也欢迎大家继续访问我们的官方网站 (Simmons & Simmons.com) 浏览收看更多的、更新的内容或者联系我们。您会在网站上看到我们的联系方式，我们希望和您有机会进一步在线下探讨。

再次感谢大家的聆听，谢谢。

simmons+simmons

For additional information on our firm, please visit our website at simmons-simmons.com.