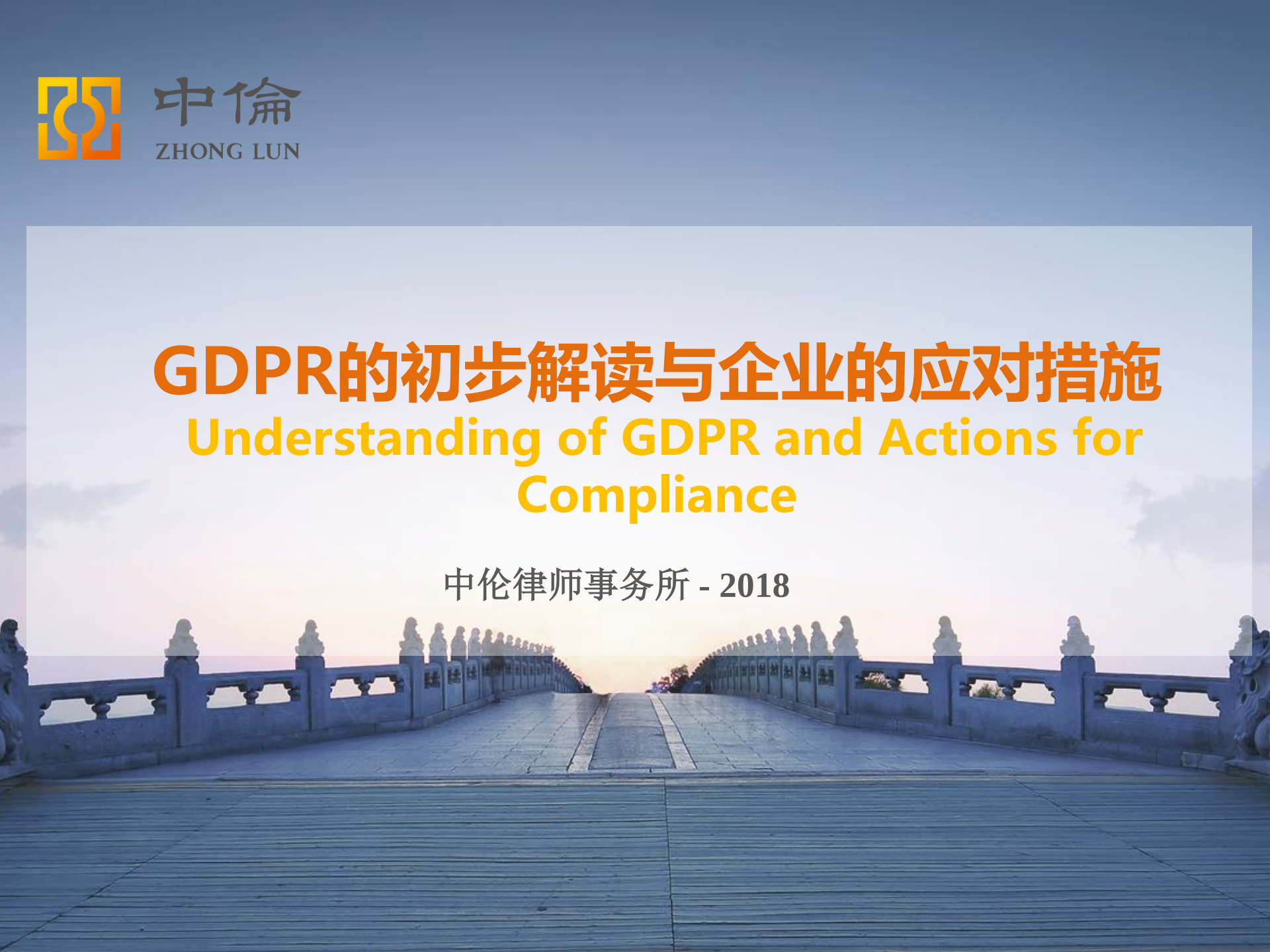
中倫
ZHONG LUN

GDPR的初步解读与企业的应对措施

Understanding of GDPR and Actions for Compliance

中伦律师事务所 - 2018



演讲人: 陈际红，合伙人

Tel : +8610 5957 2003
Fax: + 86 10 65681022
Email: chenjihong@zhonglun.com

全国律师协会信息网络与高新技术委员会，副主任;
中国互联网协会法治工作委员会，顾问;
中国法学会网络与信息法学研究院，常务理事;
国家知识产权局国家知识产权专家库，专家;
国家知识产权战略办公室，入库知识产权战略专家;
北京重点产业知识产权联盟，知识产权专家;

执业介绍

陈际红律师从1996年开始执业，为众多的国际企业提供了法律服务，并多次参与了与知识产权、电信、IT有关法律法规的研讨与立法工作，参与过的立法工作包括《计算机软件保护条例》、《电子签名法》、《著作权法》、《电信法》和《网络安全法》等。新华社、人民日报等对他的研究与律师执业做过深入报道。

陈际红律师于2005年被法制日报及中国电子商务协会联合评为“2005IT法务人年度十佳”；2006年入选国家知识产权战略办公室评选的国家知识产权战略专家； 2011年入选英国Corporate INTL Magazines 评选的“中国最佳50名律师”；2011年入选国家知识产权局评审的国家知识产权专家库；2013年陈律师被北京市律师协会授予“北京市十佳知识产权律师”的称号。2015年被ALB评选为中国最佳15名知识产权律师。2016年，被MIP（Managing Intellectual Property）评选为“中国杰出知识产权律师”（IP Stars）；被Global Law Experts评选为（2016最佳中国电信法律师）Telecommunications Law - Lawyer of the Year in China – 2016；2016-2017连续两年被Corporate INTL评选为中国年度最佳电信法律师；2018年，入选2018 World IP Review Patents & Trademarks Directory评选的WIPR 2018 Leaders；多年来连续被Chambers，Legal500，LegalBand等评级机构在IP和TMT领域推荐。

1. GDPR的适用范围

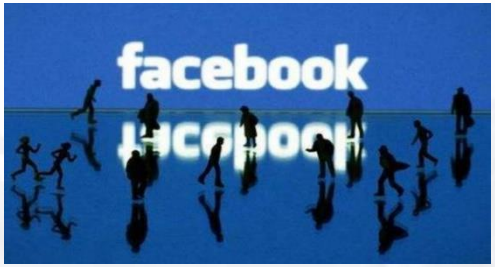
中倫 ZHONG LUN

事项范围：

- 个人数据的的自动化及非自动化处理活动；且，
- 构成文件系统一部分的个人数据处理活动；

地域范围：

- 设立于欧盟的企业从事的数据处理活动，无论其处理行为是否位于欧盟范围之内；
- 非欧盟企业：在欧盟范围内向数据主体提供商品或服务，而无论是否要求其支付对价；
- 非欧盟企业：针对欧盟范围内的数据主体的行为实施监测和追踪。



2. GDPR的救济措施及处罚

中伦 ZHONG LUN

1. 数据主体向监管机构投诉的权力；
2. 对监管机构决定的司法救济渠道
3. 通过司法途径获得赔偿的权利；
4. 行政处罚（两层次）

- 1000万欧元或企业全球营业额的2%（孰高者）；
- 2000万欧元或企业全球营业额的4%（孰高者）；
- 考虑情节：
  - 侵权行为的性质、严重程度和持续时间等；
  - 故意或过失？
  - 是否采取弥补措施？
  - 企业的安全技术措施或组织措施情况；
  - 既往违法行为；
  - 与监管机构的合作；
  - 个人数据的类型等。

风险级别的综合判断：

- **是否是大企业，涉及大量数据？**
- **是否遭受投诉；**
- **是否面临或发生数据泄露的风险？**

3. 个人数据处理应遵循的六原则

中伦 ZHONG LUN

lawfulness, fairness and transparency
合法、公正和透明原则

数据处理活动对数据主体而言应当是合法、公正和透明的

purpose limitation
目的限制原则

收集目的必须特定、明确、合法；数据处理不得违背收集目的。

data minimization
数据最小化原则

限于数据处理目的充分、相关和仅限于必需的范围之内

accuracy
准确性原则

数据必须准确、实时更新，错误数据必须及时予以删除、纠正

storage limitation
存储限制原则

存储格式应当能够用于识别已经超出收集目的的数据主体；存储期限不应超过满足数据处理目的所需的合理期限

integrity and confidentiality
完整性和保密性原则

数据处理方式应当确保个人数据安全，包括采取适当技术和组织措施，防止数据被非法或非授权处理，或者意外丢失、破坏或毁损。

3. 数据处理合法性的六情形

- 数据主体对数据处理目的表示同意；
- 系履行合同所必需，且数据主体为该合同一方当事人；或，经数据主体签约前请求的签约行动；
- 系数据控制人为履行法律义务所必需；
- 系保护数据主体或其他自然人切身利益之必需；
- 系为履行公共利益任务或公务职责所必需；
- 系为追求数据控制人或其他第三人合法权益所必需，除非此种利益应让位于数据主体的利益、基本权利或自由。

4. 数据主体同意的条件

- 能够证明的同意；
- 如是书面声明，且涉及其它事项，则同意应当通俗易懂、易于获取、与其它事项有显著的区别；
- 数据主体有权随时撤回同意；（被告知、难易度适当）
- 自由做出： 是否把履行合同绑定同意数据处理；
- 适用于儿童时，其年龄须在16岁以上，或由其监护人代为做出同意的意思表示；

5. 数据主体权利：访问权

中伦 ZHONG LUN

获取权—有权从数据控制人处获取其个人数据副本。

请求权—有权要求数据控制人采取适当安全保护措施确保数据跨境流动的安全。

知情权—有权要求数据控制人确认其个人数据是否正在被处理，获取以下信息：

1. 处理目的；
2. 数据类别
3. 被披露给的第三者；
4. 预期数据保留时间/数据保留标准；
5. 告知更正权和删除权，限制或拒绝处理权；
6. 投诉的权利；
7. 如非从数据主体收集，告知来源信息；
8. 自动化决策权权：逻辑、意义和影响。

5. 数据主体权利：更正权

中伦 ZHONG LUN

错误个人数据的改正权

指向数据控制人提出的、要求其不得不合理拖延地改正有关其本人个人数据中的错误数据的权利。

不完整个人数据的完整权

指向数据控制人提出的、要求其将有关数据主体本人个人数据中不完整的数据予以补充、完善直至达到完整的权利。

个人数据的追加权

指向数据控制人提出的、要求其对有关数据主体本人不完整数据实施数据追加或者提供数据追加声明，使其达到完整的权利。

5. 数据主体权利：删除权（被遗忘权）

中倫 ZHONG LUN

第十七条 数据主体的个人数据删除权（被遗忘权）

删除权：要求数据控制人不得不合理拖延地删除其个人数据的权利
具有下列情形之一的，数据控制人应当毫无拖延地删除个人数据

无必要继续拥有
与收集或处理目的相比，继续拥有个人数据已无必要

数据主体撤回同意
数据主体依法撤回同意数据处理的意思表示，进行数据处理尚无其他合法理由

数据主体反对数据处理
数据主体依法反对对其数据实施数据处理，进行数据处理尚无其他合法理由

数据处理活动非法
对个人数据的数据处理活动缺乏正当法律依据

删除系为履行法定义务
作为法定义务主体，删除个人数据系为履行欧盟或成员国法规定的法律义务

收集的数据系儿童数据
所收集的个人数据，系在提供信息社会服务过程中依法收集的儿童数据

数据控制人：通知后手予以删除的附加义务
个人数据已被数据控制人披露于其他数据控制人的，应数据主体要求，数据控制人在删除个人数据后，还应通知其他正在实施数据处理活动的数据控制人采取合理步骤和技术措施、兼顾可行技术和实施成本，按数据主体要求删除该个人数据的所有链接、拷贝或备份

删除权、被遗忘权排除适用的法定情形

表达自由权、信息自由权
为行使表达、信息自由权之需要

公共健康之公共利益
为保护公共健康领域的公共利益所必需

法律主张
为构建、行使或抗辩某项法律主张

法定义务、公共利益职责、法定职权
作为法定义务主体，为履行欧盟或成员国法规定的有关数据处理的法定义务，或者数据控制人为履行公共利益职责或法定职权所必需

特定领域之存档归档
为依法完成公共利益、科学和历史研究、统计分析等领域的存档目的，删除权将阻碍或妨害数据处理目标的实现

5. 数据主体权利：处理限制权

中伦 ZHONG LUN

第十八条 数据主体的个人数据处理限制权

在下列情形下，数据主体可以要求数据控制人限制其数据处理活动

- 数据主体指出其个人数据不准确，在给定的期限内要求数据控制人补正其个人数据的准确性
- 数据控制人无需继续处理个人数据，数据主体需要利用其构建、行使或抗辩某个法律主张的
- 数据处理活动非法，数据主体拒绝行使其个人数据删除权，代之以要求限制使用其个人数据的
- 数据主体反对数据处理，放弃在数据控制人数据处理合法理由与数据主体本人合法权利、利益、自由之间做出权衡，仅要求限制数据控制人的数据处理活动的

5. 数据主体权利：可携带权

中伦 ZHONG LUN

第二十条 数据主体的数据可携权

- 数据主体有权要求数据控制人以结构化、通用化、机器可读化格式提供个人数据
- 特定情形下，数据主体有权将已提供予数据控制人的个人数据无障碍地传送予其他数据控制人
- 只要技术可行，数据主体有权将其个人数据从一个数据控制人直接传送至另一个数据控制人

- 行使数据可携带权，不得损害数据主体的个人数据删除权和被遗忘权
- 数据可携带权不得适用于数据控制人为从事公共利益、履行法定职权而开展的数据处理活动
- 数据可携带权不得对他人合法权利和自由形成任何不利影响

5. 数据主体权利：反对权

中伦 ZHONG LUN

第二十一条 数据主体的数据处理反对权

数据主体：针对数据公益处理活动的反对权

针对数据控制人以公共利益、法定职权、自己或他人合法权益为由而开展的数据处理活动包括数据画像活动，数据主体有权根据自身特殊情况在任何时候向其提出反对或拒绝的权利。

数据主体：针对商业推广数据处理活动的反对权

针对以商业推广为目的的数据处理活动包括含此目的的数据画像活动，数据主体有权在任何时候向数据控制人、数据处理人提出反对或拒绝的权利。

数据主体：针对科学历史研究和统计分析目的数据处理活动的反对权

针对以科学、历史研究或统计分析为目的的数据处理活动，数据主体有权根据自身特殊情况向数据控制人、数据处理人提出反对或拒绝的权利。

数据控制人：抗辩不成功即行停止以此为由的数据处理活动

数据控制人应当举证证明其数据处理活动的法律根据和理由大于数据主体的合法利益、权利和自由或者大于构建、行使或抗辩某个法律主张。

数据控制人处理人：收到通知即行停止含此目的的数据处理活动

一经收到数据主体反对或拒绝意见，数据控制人、数据处理人应当立即停止以商业推广为目的的数据处理活动。

数据控制人处理人：以执行公益为由可以提出抗辩

数据控制人、数据处理人提出，其以科学、历史研究或统计分析为目的的数据处理活动系为开展公共利益活动所必需，则数据主体不得继续要求行使其反对权。

5. 数据主体权利：退出权

第二十二条 数据画像等涉人自动化决策分析活动

数据主体有权不受完全基于自动处理决定的约束，包括分析（如：信用评级、personal profiling）：

针对数据控制人以公共利益、法定职权、自己或他人合法权益为由而开展的数据处理活动包括数据画像活动，数据主体有权根据自身特殊情况在任何时候向其提出反对或拒绝的权利。

下列情形下数据主体不得行使其选择退出权：

系为缔结、履行数据主体与数据控制人间合同所必需

数据画像等涉人自动化决策分析活动系为缔结、履行数据主体与数据控制人间合同所必需

系由欧盟或成员国法所授权

数据控制人系欧盟或成员国法的适用主体，且其已经采取适当措施对数据主体的权利、自由和其他合法权益进行了适当保护，数据控制人开展的数据画像等涉人自动化决策分析活动系由欧盟或成员国法所授权

系经数据主体明示同意

数据画像等涉人自动化决策分析活动已经数据主体明示同意

6. 数据跨境

充分性决定（Adequat Decision）

- 对个人数据跨境流动进行充分性保护评估；
- 评估标准包括相关国际协议、国内法律规定、向独立监管机构做出的遵守数据保护规则的法律承诺等；
- 除了对国家可以作出评估外，还可以对一国内的特定地区以及国际组织的保护水平作出评估判断。

具有约束力的公司规则（Binding Corporate Rules，BCR）

- BCR协议范本规定了数据保护原则、数据主体的权利、跨国企业的责任及争议解决方式和救济措施等事项；
- 初衷是让跨国公司或者公司集团能够在公司内部进行跨境数据转移；
- 《条例》对该规则给与了正式的法律地位，并详细规定了该规则获得认可的程序和内容标准。

标准合同条款（Standard Contractual Clauses）

- 欧盟标准合同以数据主体权益保护为目的，规定了数据转移当事方和数据主体在数据保护上的权责分配关系，目前欧委会通过的三个格式合同条款仍然有效；
- 如果一国企业在与欧盟成员国企业的经济往来中使用了标准合同，承诺按照合同履行其数据保护义务，便可以认定其满足了数据保护“充分性”要求；
- 《条例》增加了成员国数据监管机构可以指定标准合同条款的渠道，但必须要经过欧委会的认可 （第63条）。

已批准的行为准则（codes of conduct）

- 数据控制者可以成立协会并提出遵守《条例》的详细行为准则（数据控制人协会）；
- 这种情形主要针对不适用于《条例》充分性决定，但从欧盟接收数据的主体（第46条）。

经批准的认证机制、封印或者标识（ approved certification mechanism,seal or mark）

- 行为准则与认证机制是条例中引入的新型的合规机制，以最大化发挥第三方监督与市场自律作用；
- 主要适用于公共机构之间的数据转移活动。

7. 数据控制着和处理者

中伦 ZHONG LUN

数据控制者

- 实施适当的技术措施和组织措施，并进行更新
  - 匿名化
  - 最小化
- 包括数据保护政策
- 经批准的行为准则 + 第三方认证，可以作为实证
- 遵循目的的必要性： 收集数量；存贮时间；数据处理的程度； 可访问性；

联合控制者

- 明确的确立义务安排；
- 确定落实满足个人数据主体权利行使的责任；

数据处理者

- 以数据控制者的名义： 数据控制者应当确保数据处理者对采取恰当的技术和组织措施提供保证；
- 不得擅自引入其他的数据处理者；

8. 数据安全：技术和组织措施

中伦 ZHONG LUN

处理过程安全性 （技术措施和组织措施）

- 匿名化或加密；
- 保证处理系统的保密性、完整性、可用性和可恢复性；
- 发生事故时，恢复可用性和获取数据的能力；
- 定期测试；

9. 数据安全：泄露通知

中伦 ZHONG LUN

发生数据泄露，数据控制者应当：

- 毫不迟延地，至少在72小时内，通知监管机构，除非泄露事件不会危机自然人的权利和自由；
- 如迟于72小时，需要附带解释延迟原因。

发生数据泄露，处理者应当即通知数据控制者；通知应包括：

- 泄露事件性质的描述，包括数据主体和数据的数量和数据类别；
- 联系方式，信息获取渠道： 数据保护专员；
- 描述信息泄露的可能情况；
- 拟采取的计划和措施，及减轻负面影响的措施。

当发生风险很高时，应当及时与数据主体进行沟通。

10. DPIA和事先沟通

中倫 ZHONG LUN

DPIA - 数据保护影响评估

- 新技术，新产品， 高风险 ： 进行DPIA
- 评估内容：
  - 所设想机制和处理目的的系统性描述；
  - 与处理目的相关的处理机制的必要性评估；
  - 对数据主体的权利和自由影响的风险评估；
  - 所设想的处理风险的举措： 保障措施，安全措施， 确保个人数据保护的机制。

事先咨询

评估结果高风险，应咨询监管机构

10. DPO及GDPR代表指定

中倫 ZHONG LUN

DPO

- 公共当局或机构实施的处理数据活动，而非法院；
- 数据处理是数据控制者或处理者的核心活动；及，
- 对数据主体进行定期和大规模的监控；

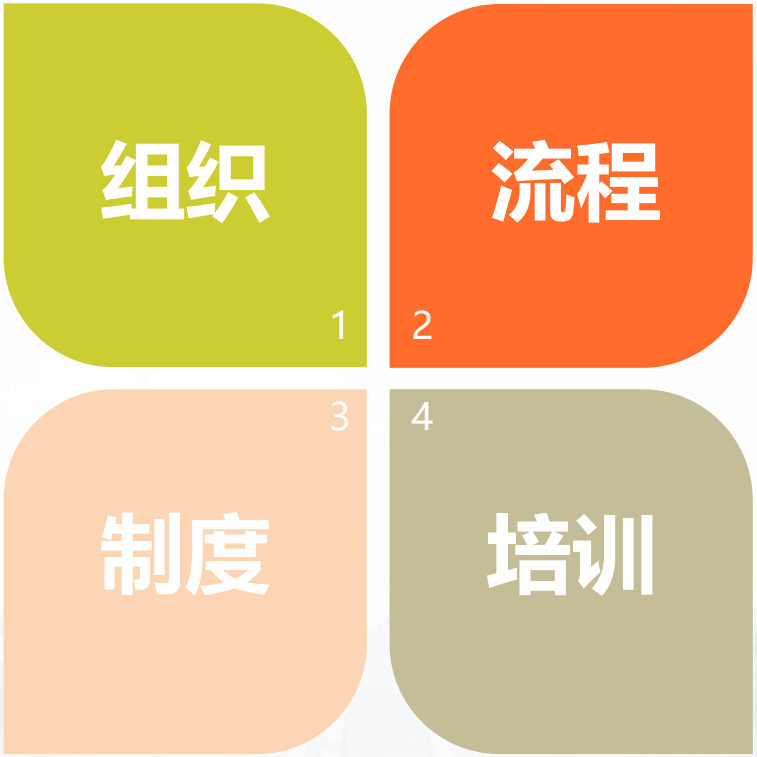
GDPR代表

- 非欧盟企业数据控制人、处理人的在欧数据代办处；
- 欧盟数据代表应当常设于一个成员国之内；
- 数据控制人、处理人指定其欧盟数据代办处，不得妨害针对其本人发起的任何法律行动；

下列情形下无须指定欧盟代表人

- 数据控制人、处理人系公共权力机关或其所属机；
- 数据处理活动偶然发生，未处理特种类型个人数据（第9条），也未处理刑事判决、违警处罚数据（第10条），不致对自然人权利和自由构成任何风险；

11. 合规实施四要素



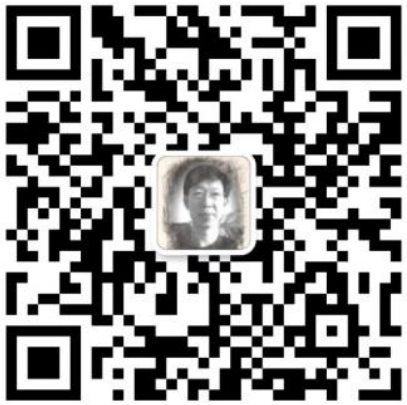
11. 网络安全合规的流程与成果
CS Compliance Workflow & Outcome

中伦 ZHONG LUN

	项目启动 Launch	尽职调查Due diligence	合规建议及合规实施 suggestions
工作流程 Workflow	制定项目计划 Project plan	1、书面尽调清单List of DD 2、尽调资料收集、阅读和分析review 3、人员访谈Interview 尽调范围包括：网络设施情况、网络安全规章制度、网络实名制、应急预案、设备采购合规、人员和资源配备、合规实施情况等。 DD scope: network facility, rules, real-name, emergency plan, purchase, staff & resources, compliance implementation	实施方案 plan 合规实施 implement 检查审核 audit 1、依据尽调制定合规实施方案 develop plan 2、完善网安规章制度 improve rules 3、制定网安制度实施流程 workflow 3、完善系统建设和设备采购流程 improve purchase flow 4、完成CII 初步识别 initial identification 5、网络安全等级保护CS MLPS 6、制度的验收、培训和提高 check,training
工作成果 Outcome	项目计划书 Prospectus	1、尽调问题清单List of DD questions 2、人员访谈计划 Interview plan 3、尽职调查报告书（分析legal gap）	1、网安实施方案 CS plan 2、全套网络安全规章制度Rules 3、完善的网络安全管理机制 mechanism 4、项目实施报告Report 5、合规培训 Training

中倫
ZHONG LUN

谢谢各位



——言中伦 行中虑——

中倫律师事务所
ZHONG LUN LAW FIRM