环球律师事务所
GLOBAL LAW OFFICE

“个人信息保护监管要求”比标分析报告

- 截至个保法草案出台

2020 年 V 1.0 版

环球律师事务所

2020 年 10 月

“个人信息保护监管要求”比标分析报告

--2020 年 V1.0 版

01

Comprehensive Analysis of Personal Information Protection Laws & Standards.

15 项个人信息保护监管要求综合分析

通过欧盟《通用数据保护条例》和中国个人信息保护相关法律法规及国家标准之间的比标，进行差异分析并提出合规思路。

02

Specific Analysis and Deep Dive of Hot Topics regarding Personal Information Protection.

5 项具体个人信息保护要求深入分析

根据本次中华人民共和国个人信息保护法（草案）的规定，我们对企业实践过程中认为非常重要的五项基本合规项进行详细分析与深入探讨，旨在引发读者更多思考及各方共同交流。

关于个人敏感信息（人脸信息）的合规治理
各国对个人敏感信息、特殊类型的数据、生物识别信息的规定上既有相同又有差异，特别对人脸信息的合规治理是当务之急。

关于告知与同意的合规要求
对于个人信息被企业收集后全生命周期的处理，各国在合法性要求思路上稍有不同，但基本上均有符合告知与同意的要求。

关于个人信息控制者与处理者合规要求
当发生对外提供个人信息时，发生“共享”和“委托处理”的情况，由此产生个人信息控制者与处理者合规要求，但称谓可能不同。

关于个人信息出境的合规治理
当发生个人信息向境外传输时，各国数据跨境的尺度与要求各有不同，具体分为“禁止跨境”、“有条件跨境”和“自由跨境”。

关于个人信息保护工作机构及负责人
当满足特定条件时，企业需要确定个人信息保护负责人/工作机构，对内负责组织实施个人信息保护工作，对外负责处理投诉等问题。

作者：

孟洁、殷坤、王程、徐晨、张淑怡、陈子谦、**D.C**

联系方式：
mengjie@glo.com.cn

目 录

前言

2020 年 10 月 21 日，《中华人民共和国个人信息保护法（草案）》（简称“《个保法草案》”）在中国人大网公布，公开征求社会公众意见。其后，将会正式出台成为我国就个人信息保护的一部位阶最高的综合性法律，标志着我国在个人信息保护方面进入 2.0 时代。《个保法草案》共八章七十条，对适用范围、个人信息处理规则、跨境传输、个人信息主体在处理活动中的权利、个人信息处理者的义务、监管部门以及罚则做出了全方位的规定，旨在对个人信息保护提供更加强有力的法律保障，同时兼顾当前社会对于数据流动与鼓励创新的需要，促进以数据为新生产要素的数字经济蓬勃发展，推动建设网络强国、数字中国、智慧社会。

《个保法草案》承袭《中华人民共和国网络安全法》（以下简称“《网络安全法》”）和《中华人民共和国民法典》（以下简称“《民法典》”）中关于个人信息保护的相关规定并对其中的规则和要求进行了细化，与其他领域的法律法规（例如《数据安全法（草案）》共同形成对我国网络安全领域立法的有力支撑，对下位法规、规则和国家标准形成有效指导。本次《个保法草案》的制定，吸收借鉴了目前国际上以欧盟《通用数据保护条例》（以下简称“GDPR”）为代表的先进立法经验，但也提出了我国特有的相关规定，不但能够顺应时代发展，还关注新需求，解决新问题。尽管《个保法草案》还处于广泛征求意见阶段，但其已体现出相关立法趋势与要求，值得企业参考并在正式发布前预先做好准备。

在《个保法草案》发布前，我国目前关于个人信息保护的规定主要是与《网络安全法》相配套的法规和国家标准。其中适用较为广泛的主要是经多次修订，并于 2020 年 3 月 6 日发布、2020 年 10 月 1 日实施的《信息安全技术 个人信息安全规范》（GB/T 35273-2020）（以下简称“《国标》”）。本报告将以 GDPR 以及我国法律法规及标准的发布时间为序，对 GDPR 以及我国在个人信息保护领域的主要法律法规、标准进行比较分析，向读者解读《个保法草案》相关规定的制定原理及相关合规建议。

本报告将分为两个部分。第一部分将基于十五个企业最关心的合规控制点作为比标维度，通过比较个人信息保护相关法规与标准的具体规定，对企业给出针对性的合规提示。第二部分将分为五个专题，例如个人信息出境等较为重要的问题进行详细分析与深入探讨，旨在引发读者更多思考以及促进共同交流。

第一部分：15 项个人信息保护监管要求综合分析

1 比标对象、方法、范围

1.1 比标分析的对象

本报告主要针对欧盟和中国在个人信息保护领域的主要法律法规、标准进行比较分析：

- 欧盟： GDPR 及 29 条工作组的相关指南；
- 中国：《网络安全法》（2016 年 11 月发布，2017 年 6 月 1 日正式实施）、《国标》（2020 年 3 月发布，2020 年 10 月 1 日正式实施，简称《国标》）、《个保法草案》（2020 年 10 月发布）。

注 1：比标法规及标准以发布时间为序。

注 2：比标项为仅覆盖同类监管要求，各法规或标准如存在特有制度或者要求的，则不作为本报告第一部分综合分析的比标项。

1.2 比标分析方法和适用范围

通过比较上述法规与标准中关于个人信息保护的具体规定，为企业给出针对性的合规提示，有利于帮助中国企业及跨国企业在中国和欧盟开展业务并处理个人信息时，识别差异、区分重点，合理建立起一套企业内部数据合规的横向基准线，提升跨司法管辖区的合规治理效率，减少重复性合规工作。特别地，在《个保法草案》发布后，有助于企业识别国内不同效力及位阶的法律法规在个人信息保护方面的要求，并制定企业内部合规指引。

2 个人信息保护立法理念

2.1 法规比标

GDPR	《网络安全法》	《国标》	《个保法草案》
以风险管理为基础框架	以用户同意为基础框架	以用户同意为基础框架	以风险管理为基础框架

2.2 合规提示

我国《网络安全法》及《国标》均采用了较为单一的以“同意”为框架的立法理念。企业对于用户的个人信息从“收集-使用-存储-分享/对外披露-销毁”的整个全生命周期的流动，都需要提前向用户告知本企业为开展某项处理活动或者提供某项服务/功能所需要向该用户收集的个人信息类型，以及用于何等目的，并且获得用户的同意。根据《国标》，如果企业向用户提供的是扩展业务功能的，在实际使用时需要用户主动开启、逐项同意，并非点击同意隐私政策文本即自动开启扩展业务功能。用户对不同意扩展业务功能，不得影响其使用产品的基本业务功能。对于个人敏感信息，企业需要对用户进行增强性告知，一般通过“弹窗”的形式进行显著提醒，并且在获得用户明示同意的情况下，才可使用和处理。

与《网络安全法》及《国标》不同，此次《个保法草案》则提出了与 GDPR 较为相似的以风险管理为基础框架的立法理念，不再采用以同意为唯一合法性事由辅以例外的模式，而是给予企业一定的风险选择空间，赋予企业更多的自主控制权和选择权，同时在违规时通过苛以高额罚款来保障权责一致性。

GDPR 根据不同风险定制了不同的义务。比如说，GDPR 提出了“特殊类型个人数据”（第 9 条和引言第 51 条），该类主体的数据因其基本权利和自由具有特别敏感性，因此企业在处理时有可能对基本权利和自由会造成显著风险，故给予特别保护。比如在收集特殊类型个人信息时，需要给予增强性的明示告知。又如，根据对个人数据识别度的从易到难，分别对已识别、可识别、去标识化和匿名化数据的合规要求，根据风险高低的不同，给予特殊保护，风险低的例如匿名化数据就不属于个人信息的范畴，无需给予特殊优待。

本次《个保法草案》也仿照 GDPR 的模式（但合法性事由并非完全一致），用六个事由概括了实践中可能出现的合法处理个人数据的情形，并考虑企业在处理个人信息时处于相对优势地位，可能给个人信息主体带来不同维度风险的情况，为企业设置了不同程度的权利、义务（第四章、第五章）。例如，根据个人信息处理的性质、范围、情境、目的，以及对个人信息主体权利和自由的不同程度和大小的风险，企业应采取合适的技术和组织方面的措施（第五章），以保证个人信息的处理能够符合法律、行政法规的规定。此外，措施应与个人信息处理的风险合乎比例（如《个保法草案》规定处理个人信息达到规定数量的，应在内部建立合适的个人

信息保护机构和个人信息保护负责人）。对于高风险的个人信息处理行为（如处理敏感个人信息、自动化决策、对外提供个人信息以及个人信息出境等），企业还应当开展个人信息安全影响评估，评估应当主动考虑风险，主动提出降低风险的方案，采取安全保护措施与风险程度相适应的模式并且据实进行记录。

《网络安全法》规定，若违反相关条款的，有可能公司会被要求责令改正、警告、没收违法所得、（最高不超过一百万人民币）罚款、停业整顿、关闭网站、吊销业务许可证或营业执照、记入社会信用档案并予以公布；对直接负责的主管人员和其他直接责任人员予以罚款；禁止从事网络服务业务等后果。

本次《个保法草案》规定的法律责任，没有改变《网络安全法》中针对单位和直接负责的主管人员、其他直接责任人员进行双罚的模式，但是由个人信息保护职责的部门要求警告、责令改正、没收违法所得之外规定了高额的罚款，并且数额可根据所涉个人信息处理行为的情节严重程度，处以五千万元以下或者上年度营业额百分之五以下的罚款，并可责令停业整顿、吊销相关业务许可证或者营业执照等。笔者初步判断，处罚力度贯彻了 GDPR 所谓的与风险相匹配原则，影响因素可能包括涉事情节、人数、后果严重性、是否采取有效补救措施等，但具体评估因素可能有待于未来正式稿以及细则的解答，建议企业予以特别重视。

3 效力和适用范围

3.1 法规比标

GDPR	《网络安全法》	《国标》	《个保法草案》
• 适用于数据控制者或处理者在欧盟**境内**的机构所进行的个人数据处理活动，而无论该处理是否发生在欧盟境内。 • 设立于欧盟**境外**的数据控制者或处理者向欧盟境内的数	适用于在中华人民共和国**境内**建设、运营、维护和使用网络，以及网络安全的监督管理。	适用于规范各类组织的个人信息处理活动，也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估。	**第三条：**适用于（1）**境内**个人信息处理者；和（2）**境外**个人信息处理者，但需满足： • 以向境内自然人提供产品或者服务为目的； • 为分析、评估境内自然人的行为；

据主体提供商品或服务或对数据主体在欧盟内的发生的行为进行监控。 • 设立于欧盟**境外**，但根据国际公法数据控制者进行的数据处理活动适用欧盟成员国法律。			• 法律、行政法规规定的其他情形。

3.2 合规提示

在大数据时代，提供产品和/或服务可能突破地域空间，企业在个人信息的处理上往往具有跨地域性，具有抽象的超越国界和领土的特质。随着数据竞争的日益激烈，各国都在试图扩大数据方面的管辖权。2018 年 3 月，美国通过《澄清域外合法使用数据法》（The Clarifying Lawful Overseas Use of Data Act, CLOUD Act，以下简称“《云法案》”），使得执法部门可依据搜查令直接调取境外数据。美国司法部对外公布的白皮书对《云法案》适用范围做出了官方解释，由此可以看出，《云法案》绝不仅仅适用于在美国注册成立的公司，境外的公司只要在经营活动中与美国有足够的联系（contacts），就可能触发美国法律的管辖权。

2019 年 11 月，欧洲数据保护委员会（EDPB）对 GDPR 第 3 条进行了统一解释，并发布了 GDPR 地域适用的指南，明确了符合“营业机构”标准或“目标指向”标准其中之一的数据处理者和控制者，均需要遵守 GDPR 规定。向欧盟居民提供服务、对欧盟居民进行监控、数据处理活动有设立在欧盟境内的营业机构进行或与其有紧密联系的情形均受到 GDPR 规制。各国为有效保障数据安全、维护国家利益，除了通过国际条约与双边/多边协议进行约定外，还通过扩大其国内法的适用范围，以求最大程度地降低跨境数据处理活动给本国带来的安全风险。因此，域外效力成为个人信息保护领域的一项立法趋势。

我国于今年 7 月份发布的《数据安全法（草案）》也逐步体现出了进行必要域外管辖趋势。本次，《个保法草案》第三条第二款明确规定，在以向境内自然人提供产品或者服务为目的，或分析、评估境内自然人的行为时，适用《个保法草案》。例如某一德国跨境电商 App 在我国大陆境内投放运营后，收集用户在使用电

商 App 过程中的个人信息，同时进行用户画像分析，即构成在我国境内收集个人信息的活动，并适用于《个保法草案》。虽然德国公司属于境外组织，其主要营业机构、数据存储服务器均不在国内，但仍有可能受到《个保法草案》和《数据安全法（草案）》的双重约束。2017 年由全国信息安全标准化技术委员会发布的《数据出境安全评估指南（征求意见稿）》曾将“境内运营”定义为在中华人民共和国境内开展业务，提供产品或服务的活动，而不论运营者是否在境内注册。另外，还提出了几项参考因素以帮助判断，包括但不限于：使用中文；以人民币作为结算货币；向中国境内配送物流等。因此，本次《个保法草案》实际上是丰满了《网络安全法》中提及的“境内运营”的理解。

然而在实务中，该条是否能得到有效的执行，又会被提出疑问，因为这些境外组织毕竟未在中国大陆境内注册设立营业机构。因此《个保法草案》第五十二条进一步规定“在中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门”，在一定程度上也是确保第三条第二款可以落地的措施之一，与 GDPR 第 27 条设定“当地代表”的思路如出一辙。虽然《个保法草案》还处于草案阶段，对于境外企业来说，建议关注域外效力这一趋势，为适用未来正式出台的个人信息保护法提前做好准备。至于境外个人信息处理者在境内的代表具体由谁来担任，以及是否可由律所或其他专业机构来担任，将有待实践中的进一步观察并期待可由个保法细则进行指引。

此外，对于境外的组织、个人，不仅适用《个保法草案》第七章规定的法律责任，同时根据第四十二条规定，如损害国内公民的个人信息权益，或者危害我国国家安全、公共利益的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。这条显然也是与《数据安全法（草案）》第二条第二款的规定相辅相承，体现了维护国家安全和数据主权的立法宗旨。但这个类似“黑名单”的限制清单如何做到日常监管与更新，本次《个保法草案》也没有明确说明，也将有待实践中的进一步观察并期待个保法细则进行指引。

4 个人信息和敏感个人信息

4.1 法规比标

GDPR	《网络安全法》	《国标》	《个保法草案》
• **个人信息**：与**已识别**出或**可被识别**的自然人相关的任何信息；可被识别的自然人指，借助标识符，例如姓名、识别号码、位置数据、网上标识符，或借助与该个人生理、心理、基因、精神、经济、文化或社会身份特定相关的一个或多个因素，可被直接或间接识别出的个人。 • **敏感信息**：处理能够揭露出其种族、民族、政治观点、宗教和哲学信仰，或工会成员身份的个人数据；处理基因数据、生物识别数据，以识别出特定个人；处理健康数据、与自然人性取向或性经历有关的数据。	• **个人信息**是指以电子或者其他方式记录的能够单独或者与其他信息结合**识别**自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。	• **个人信息**：以电子或者其他方式记录的能够单独或者与其他信息结合**识别**特定自然人身份或者**反映**特定自然人活动情况的各种信息。 • **个人敏感信息**：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。 **+ 附录 B**	• **第四条：个人信息**是以电子或者其他方式记录的与**已识别**或者**可识别**的自然人有关的各种信息，不包括匿名化处理后的信息。 • **第二十九条：敏感个人信息**是一旦泄露或者非法使用，可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息，包括种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等信息。

4.2 合规提示

我国对于个人信息概念的界定在民事、行政、刑事法角度都有涉及。具体而言：

刑事：《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（以下简称“《侵犯个人信息罪司法解释》”）第一条规

定，《刑法》第二百五十三条之一规定的“公民个人信息”是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。

民事：《民法典》第一千零三十四条规定，个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

行政：《网络安全法》中对个人信息的规定详见表格。此外，《电信和互联网用户个人信息保护规定》第四条中个人信息是指电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等信息。《个人信息和重要数据出境安全评估办法（征求意见稿）》第十七条中个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

中欧对个人信息的认定均遵从“识别”的维度，在本质上没有区别（注意匿名化以后的信息均不再视为个人信息）。识别是指从信息到个人，由信息本身的特殊性识别出特定自然人，但是不同部门法对于“识别”的内涵却经历了从“单独识别”与“结合识别”（即可识别）的过程。此外，《国标》在“识别“以外还配合了“关联”这个维度，但凡能够“反映特定自然人活动情况”的，由“特定自然人在其活动中产生的信息（如个人位置信息、个人通话记录、个人浏览记录等），即从个人到信息的情况，都视为个人信息，实则是拓宽了个人信息的认定范围，与《侵犯个人信息罪司法解释》为例的刑事角度认定标准保持一致。那么《个保法草案》是否继续维系以《网络安全法》为例的单一识别维度，还是以《国标》及刑事角度认定个人信息的范围，也是值得观察与考证的方面。但无论如何，都旨在保护自然人的个人信息权益（《个保法草案》第二条），规范个人信息的处理活动，并保障个人信息的合理利用（《个保法草案》第一条）。

对于敏感个人信息的认定，GDPR 采取列举式，《国标》和《个保法草案》则采取列举+概括式。GDPR 将敏感信息归类为个人数据中的“特别类别”，根据敏感程度的递增，处理要求与限制条件也越多。譬如，对于种族、民族、政治观点、宗教和哲学信仰，或工会成员身份的个人数据，原则上可以处理，但处理过程中不得泄露信息；基因数据、生物识别数据，原则上也可以处理，但需要对其目的予以限定；健康数据、与自然人性取向或性经历有关的数据，原则上就禁止处理。但上述的可以处理，均需要基于数据主体的同意，或者数据主体已经将该等信息公开，为建立、履行或者保护合法诉求或者为了公共利益或者与公共利益相关的归档、科学等事宜，否则仍然禁止予以处理。

在我国对于个人敏感信息（《国标》用词）或敏感个人信息（《个保法草案》用词）的表述基本一致，外加采用对定义具体举例进行阐明的方式。但实际上个人敏感信息确实还会因为其敏感程度对不同人在保护要求上会有所差别，例如有些人的 Face ID 泄露只影响其财产与身份的权益，但有些人可能会因此遭到社会压力或者被敲诈勒索而引发更为严重的身体健康甚至于生命安全问题。因此，也需要企业在不同的情境下进行风险判断并实施适当的合规措施。当然，《国标》的附录 B 的列举可以做基本参考，也是有利于企业更加轻松地完成认定。

类型列举	具体内容
个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮箱等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
个人财产信息	银行账号、存款信息、房产信息、信贷记录、征信信息、交易和消费记录、虚拟货币等虚拟财产信息……
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息

网络身份标识信息、个人教育工作信息、个人位置信息、联系人信息、个人通信信息、个人常用设备信息、个人上网记录、其他信息……

综上来看，由于认定个人信息属于一项动态过程，无论是对个人信息还是敏感个人信息的分析都建议放到具体的场景中予以考虑，能影响到个人权益的、与其他已识别的个人信息同时出现的或者组合后就可能属于被保护的范围。但是，个人信息的应用场景在扩展，其范围也可能被扩展，数据的自由流动也可能产生困难。个保法需要兼顾保护个人权益的目标，同时也要杜绝个人信息范围无限扩张进而阻碍经济与科技的正常发展。

5 个人信息处理的基本原则

5.1 法规比标

GDPR	《网络安全法》	《国标》	《个保法草案》
• 个人数据处理必须遵守**合法、公平、透明**原则。 • 个人数据收集必须符合**明确、明示、正当**的目的，处理个人数据时应与这些目的相匹配；出于公共利益、科学或历史研究目的、统计目的而对个人数据做后续处理时，在满足第 89 条第一款的前提下，可不受“目的限制原则”的约束。 • 仅仅处理目的所必需的**充分**（adequate）、**相关**的（relevant）的个人数据。避免处理额外的数据。 • 确保个人数据的准确，在有必要的情况下，确保数据时时更新；采取所有可能的、合理的措施，确保就目的来说不准确的个人数据，能够及时清除或修正。（**准确性原则**） • 仅确保实现目的所必须的时间限度内，存	• **合法、正当、必要；选择同意原则**——遵循**合法、正当、必要**的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。 • **最少够用、公开透明原则**——网络运营者**不得**收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定或者与用户的约定，处理其保存的个人信息。 • **确保安全原则**——网络运营者**应当**采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况	• **权责一致**原则——对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任。 • **目的明确**原则——具有明确、清晰、具体的个人信息处理目的。 • **选择同意**原则——向个人信息主体明示个人信息处理目的、方式、范围、规则等，征求其授权同意。 • **最少必要**原则——只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时根据约定删除个人信息。 • **公开透明**原则——以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督。 • **确保安全**原则——具备与所面临的安	• **第五条：合法正当**原则——处理个人信息应当采用合法、正当的方式，遵循诚信原则，不得通过欺诈、误导等方式处理个人信息。 • **第六条：最小必要**原则——处理个人信息应当具有明确、合理的目的，并应当限于实现处理目的的最小范围，不得进行与处理目的无关的个人信息处理。 • **第七条：公开透明**原则——处理个人信息应当遵循公开、透明的原则，明示个人信息处理规则。 • **第八条：信息准确**原则——为实现处理目的，所处理的个人信息应当准确，并及时更新。 • **第九条：归责原则**——个人信息处理者应当对其个人信息处理活动负责，

储个人数据；存储个人数据可不受上述限制而超时处理，仅当的唯一目的是出于公共利益、科学或历史研究目的、统计目的，且满足第 89 条第一款的要求。（**存储限制原则**） • 处理个人数据时应保障合适的安全水平，包括采取合适的技术或组织方面的措施避免数据遭受被授权或非法处理、意外丢失、销毁或受损。（**完整性和保密原则**） • 数据控制者负有遵循上述原则的责任，同时负有向外界表明其已经遵守上述原则的责任。（**归责原则**）	时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。 • **主体参与原则**——个人发现网络运营者**违反法律、行政法规的规定或者双方的约定**收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现**网络运营者收集、存储的其个人信息有错误的**，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。	全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性。 • **主体参与**原则——向个人信息主体提供能够访问、更正、删除其个人信息，以及撤回同意、注销账户、投诉等方法。	并采取必要措施保障所处理的个人信息的安全。 • **第十条：保护国家和公共利益原则**——任何组织、个人不得违反法律、行政法规的规定处理个人信息，不得从事危害国家安全、公共利益的个人信息处理活动。

5.2 合规提示

纵观以上基本，除了《网络安全法》的原则较为概括外，其他各法的原则总体上差异不大，其中《个保法草案》相较于《国标》，新增准确性原则和保护国家和公共利益原则，与 GDPR 的用词保持了一致。企业在欧盟法和中国《个保法草案》的语境下均需要注意“归责原则”，即对自身的数据合规行为进行“证明”。落实这一原则，有两层义务：一方面，合规义务，即企业有责任确保个人信息的处理活动符合法律和行政法规的原则和规则；另一方面，举证义务，即企业负有举证责任，需要向监管机构展示和解释其处理行为，以证明其合规。同时，企业需要知悉如果自己的不合规或者拒绝履行安全管理要求将与严厉的处罚成正比。此外，从对 GDPR 的解读来看，归责原则还要求企业设置数据保护官，记录全部数据活动，对高风险

的数据处理活动要事先进行数据保护影响评估与事先咨询，采取数据安全保障措施以及在数据泄露时，向监管机构和数据主体进行报告。可见，在一定程度上，“归责原则”所蕴含的层次比起《国标》的“权责一致”原则，更加丰富和饱满。

此外，《民法典》中也有对个人信息保护原则的相关规定，比如第一千零三十五条规定了处理个人信息需要遵循合法、正当、必要原则，并符合选择同意原则、目的明确、公开透明原则；第一千零三十七条规定主体参与原则；第一千零三十八条要求确保安全原则，只是在具体原则的表达和措词上可能略有不同，比如自然人可以依法向信息处理者查阅或者复制其个人信息，而《国标》的用词则为个人信息有访问及获取个人信息副本权。

6 收集和处理个人信息的正当性事由

6.1 法规比标

GDPR	《网络安全法》	《国标》	《个保法草案》
数据主体对出于单个或多个特定目的而处理其个人数据表示**同意**； 处理是为向身为合同当事人之数据主体**履行合同**所必须的，或在缔约前，应数据主体的要求所必须采取的步骤； 因履行数据控制者承担的**法律义务**而必须处理个人数据的； 为保护数据主体**重大利益**或其他自然人重大利益而必须处理个人数据的； 为**公共利益**而执行任务，或数据控制者履行	仅有同意。	• **仅有同意：** 个人信息=》授权同意 个人敏感信息=》明示同意 **但规定了下列例外情形：** • 与个人信息控制着履行法律法规规定的义务相关的； • 与国家安全、国防安全直接相关的； • 与公共安全、公共卫生、重大公共利益直接相关的； • 与刑事侦查、起诉、审判和判决执行等直接相关的； • 出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的；	**第十三条：**符合下列情形之一，个人信息处理者方可处理个人信息： • 取得个人的**同意**； • 为订立或者履行个人作为一方当事人的**合同所必需**； • 为履行法定职责或者**法定义务**所必需； • 为应对**突发公共卫生事件，或者紧急情况**下为保护自然人的生命健康和财产安全所必需； • 为**公共利益**实施新闻报道、舆论监督等行为在合理的范

被赋予的**公共职能**时，必须处理个人数据的； 因数据处理者**正当利益**或第三方正当利益而必须处理个人数据的，但当数据主体的利益或基本权利和自由（特别当数据主体尚未成年时）高于上述正当利益时，不得使用该事由。		• 所收集的个人信息是个人信息主体自行向社会公众公开的； • 根据个人信息主体要求签订和履行合同所必需的； • 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道； • 维护所提供的产品或服务的安全稳定运行所必需的，例如发现、处置产品或服务的故障； • 个人信息控制者为新闻单位且其在开展合法的新闻报道所必需的； • 个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的；	围内处理个人信息； • 法律、行政法规规定的**其他**情形。

6.2 合规提示

GDPR 第六条提出了六种正当性事由：包括数据主体的同意、履行合同、履行法定义务、保护数据主体重大利益、公共利益以及数据控制者的正当利益。尽管在实践中，同意仍然是欧洲企业进行用户个人数据处理合法性基础的主要选择，但是除同意外，GDPR 的其他几种合法性基础也体现了立法者在多种利益冲突之间的平衡观念，赋予企业更多证明其处理活动合法性的空间，有不少企业承担一定的证明责任后，开始运用除同意以外的正当事由来证明合法事由了。

与《网络安全法》与《国标》要求以“同意”为唯一合法事由相比，本次《个保法草案》借鉴了 GDPR 第六条的体例，将日常生活中可能出现的另外五类情况（例

如履行合同所必需、履行法定职责所必需、维护公共利益），与个人信息主体的“同意”并行放置，作为处理个人信息的合法依据。只要企业证明自己具有《个保法草案》要求的合法性基础，又履行了基本的合规义务，即能够满足合规要求，这样给予企业在无法拿到“同意”时更加灵活和自我控制风险和自证合规的做法，确保企业生产运营的合规以及通过自律监管的方式保证生产要素的有效流通，两者达到平衡。

此外，《个保法草案》没有 GDPR 中的为保护数据主体或者其他自然人的重大利益而必须处理个人数据的选项，但它结合了近期 COVID-19 这类突发公共卫生事件，将紧急情况下对自然人生命健康和财产安全保护所必需增添进合法性事由，更贴近民生和实事。对于《个保法草案》为何没有采纳 GDPR 中的正当利益，笔者探究，因为数据控制者或者第三方的正当利益（例如直接营销、防范欺诈、集团内部管理、网络信息安全、报告犯罪等）的存在应当经过谨慎的评估，并且需要平衡个人信息主体对隐私的合理期待，否则数据主体的利益和基本权利是需要显著优先于数据控制者的利益的（GDPR 引言第 47 条）。因为 GDPR 对平衡条款的设置比较成熟，因此企业对正当利益的把握较为容易，但我国法律原先是遵循“同意”为基础框架的路径，从《个保法草案》开始改为以风险管理和平衡为基础框架，实则需要一定的适应过程，可能很多企业在一开始还不一定能够很好把握，如果马上让其自我平衡“正当利益”可能会适得其反，还不如通过法律、行政法规规定的其他情形这类我国常见的兜底条款，从而在未来能够通过制定司法解释或者细则等进行调适。

7 获得信息主体“同意”的要求

7.1 法规比标

GDPR	《网络安全法》	《国标》	《个保法草案》
“同意”：数据主体基于其意思，通过声明或明确肯定的行动，所表示的**自主、具体、知情及明确**的处理与其个人数据有关的同意。	/	“明示同意”：个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主作 出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。	• **第十四条：**处理个人信息的同意，应当由个人在**充分知情**的前提下，**自愿、明确**作出意思表示。法律、行政法规规定处理个人信息应当取

当处理是基于同意时，数据控制者应证明数据主体已同意对其个人数据的处理； 如数据主体做出的书面同意声明涉及其他事项，同意请求应以与其他事项清楚区分的方式呈现，并采取易懂且方便取得的形式，采用清楚简易的语言。任何违反 GDPR 的声明条款都不具有约束力。 评估同意的作出是否具有自主性时应特别考虑，合同的履行是否将同意不作为履行合同必需的条件。		注:肯定性动作包括个人信息主体主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填 写或提供等。 需要**明示**同意的情形如下： • （1）收集个人敏感信息； （2）收集不满 14 周岁未成年人个人信息前，应征得其监护人的明示同意； （3）如开展业务所需进行的个人信息处理活动超出已获得的授权同意范围的， 应在获取个人信息后的合理期限内或处理个人信息前，征得个人信息主体 的明示同意，或通过个人信息提供方征得个人信息主体的明示同意； （4）因业务需要，确需共享、转让的， 应单独向个人信息主体告知目的、涉及的个人生物识别信息类型、数据接收方 的具体身份和数据安全能力等，并征得个人信息主体的明示同意； （5）信息控制者发生收购、兼并、充足、破产等变更后，变更后的个人信息控制者应继续履行原个人信息控制者的责任和义务，如变更个人信息使用目的时，应重新取得个人信息主体的明示同意；	得个人**单独**同意或者**书面**同意的，从其规定。 • **第十五条：**个人信息处理者知道或者应当知道其处理的个人信息为不满十四周岁未成年人个人信息的,应当取得其监护人的同意。 • **第十七条：** 个人信息处理者不得以个人不同意处理其个人信息或者撤回其对个人信息处理的同意为由,拒绝提供产品或者服务;处理个人信息属于提供产品或者服务所必需的除外。

		（6）经法律授权或具备合理事由公开披露时，应向个人信息主体告知公开披露个人信息的目的、类型，并事先征得个人信息主体明示同意。	

7.2 合规提示

GDPR 下数据主体的同意：数据主体通过书面声明或经由一个清楚确定的动作，表示同意对其个人数据进行处理。该意愿表达应是自由给出的（freely given）、特定的（specific）、显示出数据主体对前因后果清楚的（informed）、清晰明确的（unambiguous）数据主体的权利。对数据处理的要求应当与其他事项明确、明显地区别开，同时使用清晰、直白的语言，以可理解的、易于接触（accessible）的形式呈现。如果声明包含了与该规定不符的内容，则不符部分无效。数据主体有权在事后撤回其同意，但撤回同意不影响同意撤回前数据处理的合法性。在表达同意前，数据主体应被告知其有权随时撤回同意，并且，撤回同意应与表达同意同样方便。

根据《网络安全法》第四十一条和《民法典》第一千零三十五条，处理个人信息的法律依据以个人信息主体同意为原则，其他法律法规规定为例外。《国标》则以同意为原则，并列举了处理个人信息不必征得个人信息主体同意的情形，包括履行合同所必需、履行法定义务等。《国标》中的同意，虽然没有 GDPR 要求的这么细致，但是也是要求通过肯定性动作做出明确授权，包括了 explicit+ unambiguous 两方面要素，也说明用户只能选择同意（Opt-in）, 不能选择退出（Opt-out）。

《国标》不但将需要用户明示同意的情形做了明确规定（如上表），而且对基本业务功能与附加业务功能中的敏感信息告知同意方式进行了细分。比如基本业务功能的，个人信息主体告知基本业务功能所必要收集的个人信息类型，以及个人信息主体拒绝提供或拒绝同意收集将造成的影响，并通过个人信息主体对信息收集主动作出肯定性动作（如勾选、点击“同意”或“下一步”等）征得其明示同意；应允许个人信息主体选择拒绝提供其个人信息。对于产品或服务如提供扩展业务功能的，在扩展业务功能首次使用前，应通过交互界面或设计（如弹窗、文字说明、填写

框、提示条、提示音等形式），向个人信息主体逐一告知所提供扩展业务功能及所必要收集的个人信息，并允许个人信息主体对扩展业务功能逐项选择同意。当个人信息主体拒绝时，个人信息主体不同意收集扩展业务功能所必要收集的个人信息的，个人信息控制者不应反复征求个人信息主体的同意（48 小时内不得重复）。实际上，《国标》对同意机制的设置是相对较精细的，《个保法草案》第十七条实则也做了回应，“个人信息处理者不得以个人不同意处理其个人信息或者撤回其个人信息处理的同意为由，拒绝提供产品或者服务，但处理个人信息属于提供产品或者服务所必需（核心业务功能）的除外”。但是，笔者也担心《个保法草案》的修改可能对企业原本以同意为机制的产品设计逻辑产生重大影响，是否意味着未来企业需要为不同的处理活动确定不同的法律依据，以及企业是否可以在论证和选择法律依据的问题上有一定的空间，可能有待未来个保法正式稿或者细则进一步解答。

此外，《个保法草案》规定了个人信息主体作出同意的构成要件，即应当由个人在充分知情的前提下，自愿、明确地作出意思表示。同时《个保法草案》还提出了“单独同意”和“书面同意”的概念，其中需要单独同意的场景包括：

（1）个人信息处理者向第三方提供其处理的个人信息的，应当向个人告知第三方的身份、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。（《个保法草案》第二十四条）

（2）基于个人同意处理敏感个人信息的，个人信息处理者应当取得个人的单独同意。法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。（《个保法草案》第三十条）

（3）个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的身份、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式等事项，并取得个人的单独同意。（《个保法草案》第三十九条）

（4）取得个人单独同意或者法律、行政法规另有规定的，个人信息处理者方可公开其处理的个人信息。（《个保法草案》第二十六条）

（5）取得个人单独同意或者法律、行政法规另有规定的，所收集的个人图像、个人身份特征信息方可公开或者向他人提供。（《个保法草案》第二十七条）

从以上需获得单独同意的情形观察，总体上处理行为具有更高的风险，也可能涉及个人敏感信息，需要通过强提示，让个人信息主体充分知悉风险，经过审慎地思考并通过主动勾选或者签署等肯定性的动作，作出自己充分的意思表达，而不得通过概括授权的方式代替而日后主张不知情或者未尊重用户选择。但是，具体如何分别满足“单独同意”或“书面同意”的要求，以及这两者是否就一定是等效的，也有待未来正式稿进一步解答。

对于儿童个人信息的年龄线，中欧规定稍有差别。GDPR 规定的儿童年龄为 16 岁以下，但不得低于 13 岁；《国标》及《个保法草案》规定的儿童为未满 14 周岁的自然人。收集儿童的个人信息，均需要取得其法定代理人（或监护人）的授权或同意。根据不完全考证，我国将儿童的年龄定为 14 周岁的法规可能是 2013 年国务院关于修改《全国年节及纪念日放假办法》的决定，规定不满 14 周岁的少年儿童可以在 6 月 1 日儿童节当天放假 1 天；14 周岁以上的青年在 5 月 4 日青年节当天放假半天。目前，无论是《数据安全管理办法（征求意见稿）》还是《儿童个人信息网络保护规定》，我国均将儿童的年龄定格在 14 周岁以下。处理儿童个人信息的，应当征得儿童监护人的同意。本次《个保法草案》还对儿童的界定采用了推定知情的方式，则个人信息处理者知道或者应当知道其处理的个人信息为不满十四周岁未成年个人信息的，一定程度上要求企业不得开脱自身的责任，比如游戏类公司，在注册时需要采取实名制认证的，那么该企业就不得借口自己不知道使用者为儿童而逃避征得监护人同意的义务。应当知道，也表示如果游戏企业未采取实名制认证的，也是没有达到法律的要求。

8 个人信息主体的权利实现

8.1 查询权

GDPR	《网络安全法》	《国标》	《个保法草案》
数据主体有权从控制者处获得关于其个人数据是否被处理的确认回复，如确定个人数据正被处理，则数据主体有权获得如下信息：	/	个人信息控制者应向个人信息主体提供访问下列信息的方法： • 其所持有的关于该主体的**个人信息或类型**；	**第四十五条：**个人有权向个人信息处理者**查阅**其个人信息，但有《个保法草案》第十九条第一款规定的情形（法律、行政法规规定应当

• 处理的**目的**； • 涉及个人信息的**类别**； • 个人数据的（包括将来可能的）**接收者、接收者的类别**，特别是位于第三国的接收者或国际组织； • 数据将会存储的**期限**，如无法明确，则列出决定存储期限的标准； • 数据主体的**各项权利**，如修正或删除个人数据的权利、限制个人数据处理的权利、反对处理的权利； • 向监管部门**申诉**的权利； • 如数据并非从数据主体处收集而得，则关于数据**来源**的信息； • 告知数据主体是否采用了第 22 条（1）和（4）规定的**自动化决策机制**，包括数字画像，并提供关于自动化决策机制有意义的信息，以及根据设想对数据主体将造成的影响。		• 上述个人信息的**来源**、所用于的**目的**； • 已经获得上述个人信息的**第三方身份或类型**。 注：个人信息主体提出访问非其主动提供的个人信息时，个人信息控制者可在综合考虑不响应请求可能对个人信息主体合法权益带来的风险和损害，以及技术可行性、实现请求的成本等因素后，做出是否响应的决定，并给出解释说明。	保密或者不需要告知的情形）除外。 个人请求查阅其个人信息的，个人信息处理者应当及时提供。

8.2 更正权

GDPR	《网络安全法》	《国标》	《个保法草案》
数据主体应当有权要求数据控制者无不当迟延的**更**	个人发现网络运营者收集、存储的其	个人信息主体发现个人信息控制者所持有的该主体	**第四十六条：**个人发现其个人信息不准确或者

正与该数据主体相关的不准确个人数据。考虑到处理的目的，数据主体有权**完善**其尚不完整的个人数据，包括以提供补充说明的方式。	个人信息有错误的，有权要求网络运营者予以**更正**。网络运营者应当采取措施予以更正。	的个人信息有错误或不完整的，个人信息控制者应为其提供请求**更正**或**补充**信息的方法。	不完整的，有权请求个人信息处理者**更正、补充**。个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以**核实**，并及时更正、补充。

8.3 删除权

GDPR	《网络安全法》	《国标》	《个保法草案》
符合以下情形的，个人信息主体要求删除的，**应及时**删除个人信息： • 对收集或以其他方式处理个人数据所服务于的目的来说，该个人的数据不再是必需的； • 对数据处理是基于同意时，且不基于其他法律基础时，数据控制者撤回其同意的； • 数据主体反对根据正当利益开展的处理，同时数据控制者没有其他高于数据主体利益的、正当的理由继续数据处理，或数据主体反对直接市场营销时； • 个人数据被非法处理； • 根据欧盟、成员国法律要求，需要删除个人数据的；	个人发现网络运营者**违反法律、行政法规的规定或者双方的约定**收集、使用其个人信息的，有权要求网络运营者删除其个人信息。网络运营者应当采取措施予以删除。	符合以下情形的，个人信息主体要求删除的，应及时删除个人信息： • 个人信息控制者**违反法律法规规定**，收集、使用个人信息的； • 个人信息控制者**违反了与个人信息主体的约定**，收集、使用个人信息的。 个人信息控制者违反法律法规规定或违反与个人信息主体的约定向第三方共 享、转让个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止共享、转让的行为，并通知第三方及时删除; 个人信息控制者违反法律法规规定或违反与个人信息主体的约定，公开披露个人信息，且个	**第四十七条：**有下列情形之一的，个人信息处理者应当主动或者根据个人的请求，删除个人信息： • **约定的保存期限已届满或者处理目的已实现；** • **个人信息处理者停止提供产品或者服务；** • **个人撤回同意；** • **个人信息处理者违反法律、行政法规或者违反约定处理个人信息；** • 法律、行政法规规定的其他情形。 法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，

• 出于对未成年人保护的； 在以下情形中，删除权将不予适用： • 涉及到言论自由和信息自由的； • 根据欧盟、成员国法律规定要求处理的个人数据，或为追求公共利益，或履行数据控制者负有的公共管理任务，需要处理个人数据的； • 为追求公共卫生领域的公共利益的； • 出于公共利益、科学或历史研究、统计目的等需处理个人数据的； • 关于法律诉求的建立、行使和保护。		人信息主体要求删除的，个人信息控制者应立即停止公开披露的 行为，并发布通知要求相关接收方删除相应的信息。	个人信息处理者应当停止处理个人信息。

8.4 可携带权

GDPR	《网络安全法》	《国标》	《个保法草案》
存在以下情形的，数据主体有权从数据控制者获得关于其个人数据（仅限其向数据控制者提供的）的**副本**；副本应以结构化、普遍使用、可机读的形式；数据主体有权要求数据控制者将其个人数据向其他数据控制者提供：	/	根据个人信息主体的请求，个人信息控制者应为个人信息主体提供获取以下类型个人信息副本的方法，或在技术可行的前提下直接将以下个人信息的副本传输给第三方： • 个人基本资料、个人身份信息；	**第四十五条：**个人有权向个人信息处理者复制其个人信息，但有法律、行政法规规定应当保密或者不需要告知的情形的除外。 个人请求复制其个人信息的，个人信息处理者应当及时提供。

• 数据处理是基于同意，或基于第 6 条第一款 b）项所指涉的合同 • 数据处理以自动化的形式进行。 如技术上可行的话，数据主体有权要求数据控制者将其个人数据直接**传输**给另一数据控制者。 行使该权利不应对他人的权利和自由造成不利影响。		• 个人健康生理信息、个人教育工作信息。	

8.5 自动化决策

GDPR	《网络安全法》	《国标》	《个保法草案》
当决定能对数据主体产生法律效果，或对其有显著影响时，数据主体有权不受仅仅根据自动化数据处理而作出的决定，包括数字画像。（类似于 opt-out） 当有以下情形时，上述权利不适用： • 数据处理是数据主体和控制者签署、执行合同所必需的； • 欧盟、成员国法律许可、且明确了保护数字主体权利、自由、正当利益的措施的； • 基于数据主体明确的同意。	/	当仅依据信息系统的自动决策而做出显著影响个人信息主体权益的决定时（例如基于用户画像决定个人信用及贷款额度，或将用户画像用于面试筛选），个人信息控制者应向个人信息主体提供申针对自动决策结果的投诉渠道，并支持对自动决策的人工复核。	**第二十五条：**利用个人信息进行自动化决策，应当保证决策的透明度和处理结果的公平合理。个人认为自动化决策对其权益造成重大影响的，有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。 通过自动化决策方式进行商业营销、信息推送,应当同时提供不针对其个人特征的选项。

对本条第二款 a）和 c），数据控制者应采用合适的措施，保护数字主体权利、自由、正当利益；措施至少包括数据主体有权要求控制者人工干预自动化处理，以及表达个人意见、对决定提出抗辩的权利。 对第 9 条 1）款列出的特别类别的个人数据，自动化决定不应根据上述数据而作出；例外情况是第 9 条第 2 款的(a) 或 (g) 。			

8.6 其他权利

GDPR	《网络安全法》	《国标》	《个保法草案》
限制数据处理（相当于冻结） • 数据主体对数据的准确性提出异议时； • 数据处理为非法，而数据主体反对清除其数据而是要求限制对数据的使用的； • 数据控制者出于特定目的不再需要数据主体的个人数据，但数据主体需要这些数据以建立、行使和保护自己的法律诉求的； • 数据主体反对根据正当利益的数据处理，但尚不清楚数据控制者是否有高	/	**个人信息主体撤回同意** • 应向个人信息主体提供方法撤回收集、使用其个人信息的授权同意的方法。撤回同意后，个人信息控制者后续不得再处理相应的个人信息； • 应保障个人信息主体拒绝接收基于其个人信息推送的商业广告的权利。对外共享、转让、公开披露个人信息，应向个人信息主体提供撤回同意的方法。 注：撤回同意不影响撤回前基于同意的个人信息处理。	**第十六条：撤回同意** • 基于个人同意而进行的个人信息处理活动,个人有权撤回其同意。 **第四十四条：知情权、决定权** • 个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。 **第四十八、四十九条：响应信息主体的请求**

于数据主体利益的正当事由。 反对数据处理（相当于对控制者的判断提出反对意见） • 基于其特定的情况，数据主体有权在任何时候反对基于正当利益的个人数据处理，数据控制者应停止处理，除非数据控制者能表明其有显著的正当事由，该正当事由大于数据主体的利益、权利、自由，或大于法律诉求的建立、行使和保护。【反对后，可限制，符合条件要求删除】 • 当数据处理是基于直接的市场营销目的。【反对后可直接要求删除】 当数据处理是出于科学或历史研究、数据统计时，数据主体根据其特殊情况，有权反对处理其个人数据，除非处理是为公共利益所必须。		**个人信息主体注销账户** • 通过注册账户提供服务的个人信息控制者，应向个人信息主体提供注销账户的方法，且该方法应简便易操作； • 受理注销账户请求后，需要人工处理的，应在承诺时限内（不超过 15 个工作日）完成核查和处理； • 注销过程如需进行身份核验，要求个人信息主体再次提供的个人信息类型不应多于注册、使用等服务环节收集的个人信息类型;d) 注销过程不应设置不合理的条件或提出额外要求增加个人信息主体义务，如注销单个账户视同注销多个产品或服务，要求个人信息主体填写精确的历史操作记录作为注销的必要条件等; • 注销账户的过程需收集个人敏感信息核验身份时，应明确对收集个人敏感信息后的处理措施，如达成目的后立即删除或匿名化处理等; • 个人信息主体注销账户后，应及时删除其个人信息或匿名化处理。因法律规规定需要留存个人信息的，不能再次将其用于日常业务活动中。	• 个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。 • 个人信息处理者应当建立个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。

		响应个人信息主体的请求 • 在验证个人信息主体身份后，应及时响应个人信息主体基于 8.1-8.6 提出的请求，应在三十天内或法律法规规定的期限内作出答复及合理解释，并告知个人信息主体外部纠纷解决途径; • 采用交互式页面(如网站、移动互联网应用程序、客户端软件等)提供产品或服务的，宜直接设置便捷的交互式页面提供功能或选项，便于个人信息主体在线行使其访问、更正、删除、撤回授权同意、注销账户等权利; • c)对合理的请求原则上不收取费用，但对一定时期内多次重复的请求，可视情收取一定成本费用; • 直接实现个人信息主体的请求需要付出高额成本或存在其他显著困难的，个人信息控制者应向个人信息主体提供替代方法，以保障个人信息主体的合法权益。	

8.7 权利的例外

GDPR	《网络安全法》	《国标》	《个保法草案》
欧盟、成员国法律可对数据主体第 12 条至 22 条、第 34 条赋予的权利作出限	/	• 与个人信息控制者履行法律法规规定的义务相关的；	/

制，当限制尊重基本权利和自由的实质，同时又是下列目标所必须的、成比例的： • 国家安全 • 国防 • 公共安全 • 预防犯罪、刑事侦查和起诉、处罚执行 • 其他公共利益的重要目标，特别是欧盟或成员国的重要经济、金融利益，包括财政、预算、税收、公共卫生、社保 • 保护司法独立和庭审程序 • 对受管制的行业，调查、起诉违背职业道德 • 实现上述目标时所需的监测、检查、规制 • 保护数据主体，或其他人的权利和自由 • 执行民事诉求		• 与国家安全、国防安全直接相关的； • 与公共安全、公共卫生、重大公共利益直接相关的； • 与刑事侦查、起诉、审判和执行判决等直接相关的； • 个人信息控制者有充分证据表明个人信息主体存在主观恶意或滥用权利的； • 出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的； • 响应个人信息主体的请求将导致个人信息主体或其他个人、组织的合法权益受到严重损害的； • 涉及商业秘密的。	

8.8 合规提示

在用户权利方面，国内外法规的要求基本上是类似的，都赋予了个人信息主体行使其查询、更正、删除、可携等权利。只是 GDPR 对权利实现方面说明地更加详细些，僻如，对查询的范围作出细致的规定；对于删除权，GDPR 要求控制者无条件满足，除非个别特殊情况除外（如为了公共利益、言论自由、科学研究等目的），在不存在数据处理目的或者数据主体撤回同意、拒绝处理时，需要将数据完全删除；在可携权方面，不仅包括数据控制者应当提供正在处理的个人数据副本，还包括了一方数据控制者有可能会被要求将数据传输给另一方数据控制者；对用户

画像、自动化决策机制作出了严格限制；同是，还全面考虑了用户权利的例外情形。《国标》在个别权利（如被删除权、可携带权以及用户画像）上稍有差别，没有规定被遗忘权、限制数据处理权，但规定了撤回同意和注销账户的权利，除此以外，基本上规定地比较类似。

《网络安全法》没有对用户权利进行规定，《民法典》第一千零三十七条的规定也是较为简略的。本次《个保法草案》与 GDPR 和《国标》的规制思路基本也是一致的，只是在用词上较为简练，权利层次上偏原则性一些，也没有新设内容。但有三点值得提出：首先，对于行使删除权的前提条件，《国标》要求存在违法违约情形，《个保法草案》则在此基础上新增约定的保存期限届满或者处理目的已实现、个人信息处理者停止提供产品或者服务，以及个人撤回同意时的情形。虽然这几点在《国标》的个人信息存储、停止运营以及撤回同意章节也有相关要求，但《个保法草案》进行了完整的归类，让企业更加明确地了解需要删除数据的各类场景。

其次，在可携权章节没有写入需向另一方传输数据，这可能更加符合当前国内大部分企业在制度和技术上尚未达到该要求的水平，如果一味按照 GDPR 的可携权标准，有可能将法律规定架空，实际履行变得困难，还不如在时机成熟时再提出。

其三，《个保法草案》第四十四条提出了个人信息主体除了知情权与决定权以外的限制处理个人信息和拒绝个人信息处理的权利，以及根据第四十八条有权要求企业进行解释说明的权利。GDPR 中，拒绝权属于一类机制平衡的条款（GDPR 第 21 条及引言 69 条），更多地用于平衡企业在遇到正当利益或者为了公益而处理个人数据时，个人是否仍然可以有权拒绝处理其个人数据，这里需要进行评估以及举证证明。限制处理权也需要控制者有一系列的措施来保证既符合规范又确保运营稳定。目前《个保法草案》提出的用意是好的，但是在没有细则指引的情况下，在运用的维度上可能也会五花八门，导致企业与个人信息主体各执一词。关于要求企业进行解释的权利，是否可用书面 Q&A 的格式解释方式还是需要配有专门人员进行解释，以及这些是否会增加企业成本，如何达到平衡，都是正式稿或者细则后面需要进一步考虑的问题。

实践中，这些权利不仅需要在企业的隐私政策中做出具体体现，而且需要与产品设计相结合，真正落实 privacy by design and by default，让用户实现其对个人信息

的知情权、参与权与控制权。因此，建议企业在《隐私政策》/《个人信息保护政策》中告知个人信息主体拥有查询权、更正权、删除权、复制权、拒绝自动决策、限制处理和拒绝处理权，并告知该权利的使用方法。在细节处理上，可参考并结合《国标》与《个保法草案》不存在矛盾但更具体、细化的要求，譬如，查询范围包括企业持有的关于该主体的个人信息或个人信息的类型；上述个人信息的来源、所用于的目的；以及已经获得上述个人信息的第三方身份或类型；告知删除、撤回授权的使用方法；保障个人信息主体拒绝接收基于其个人信息推送商业广告的权利。同时，推荐企业直接在产品或服务提供的功能界面中（例如 App 可设置专门的选项、功能、界面等）设置相应的机制，便于个人信息主体在线行使权利。

此外，建议企业在用户撤回授权同意后，后续不应继续处理相应的个人信息，在删除用户个人信息后，需要做到后台同步并不得再利用其已删除的个人信息进行展示或者推送。如果是利用个人信息主体的兴趣爱好、消费习惯等特征进画像和个性化展示的，建议企业保障个人信息主体有权拒绝接收基于其个人信息的推送和对其个人信息进行处理，需要给个人信息主体退出权利（拒绝关闭选项）。另外，建议企业提前考虑运营成本，根据《个保法草案》，向个人信息主体提供副本或者被要求复制其个人信息的范围已经扩展到了个人信息主体的全部个人信息了，而不局限于《国标》中所述的仅可要求获取个人基本资料、个人身份信息、个人健康生理信息、个人教育工作信息这四类。

《个保法草案》没有像 GDPR 一样涉及基于用户画像（profiling）的一般决策和基于自动化的决策（automated decision-making）两类，而是规定了利用个人信息进行自动化决策这一类（笔者猜测可能立法者仅考虑了电商领域内“大数据杀熟”这一种情况）。《个保法草案》第二十五条规定，自动化决策应当保证过程的透明与结果的公平，个人信息主体有权要求个人信息处理者说明并有权拒绝自动化决策作出的决定。并且，要求通过自动化决策所作的个性化展示需要同时提供不针对个人特征的选项。《中华人民共和国电子商务法》正有此规定，要求电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的，应当同时向该消费者提供不针对其个人特征的选项，也正印证了笔者前述的猜测。虽然有上述规定，但与 GDPR 的立法相比，《个保法草案》在该条的设计上显然还是略显粗糙，建议增加基于画像作决策的一般情况；自动化决策不得针对儿童、增加个人信息主体的控制机制，如提供隐私权设置（Privacy Settings）；如果个人信息主体撤

回同意后，不得再利用其个人信息进行画像或者推送等规定。此外，也建议个保法的正式稿可以多考虑几种场景下个性化展示/推送的情况，以更好地保护个人信息主体的合法权益，并与《国标》、《数据安全管理办法（征求意见稿）》中关于画像、自动化决策、个性化展示等内容进行协调并作好统领各法规在该事项上的作用。

最后，虽然《个保法草案》没有提起注销账号的权利，但还是建议企业不可掉以轻心，仍然应该为个人信息主体提供注销账户的方法，并在个人信息主体注销账户后，应及时删除其个人信息或做匿名化处理，在这点上尽量靠近《国标》的要求。《个保法草案》第四十八条还要求建立个人行使权利的申请受理和处理机制，这基本上可以通过《国标》所要求的及时响应个人信息主体的请求来满足。通常来说，建议企业在验证个人信息主体身份后，及时响应个人信息主体的所有合法请求包括查询、更正、删除权撤回授权同意、注销账户等。建议公司在三十天内或法律法规规定的期限内作出答复及合理解释，如果是关于 App 的请求或者进行申诉，则应在十五个工作日内完成核查和处理，包括验证身份、作出答复及合理解释，并告知个人信息主体外部纠纷解决途径。

9 数据安全能力的要求

9.1 法规比标

GDPR	《网络安全法》	《国标》	《个保法草案》
考虑到各国国内发展水平、实施成本和数据处理的性质、范围、内容和目的以及对自然人权利与自由带来风险的可能性与严重性， 数据控制者和处理者应当实施适当的技术和组织措施以确保安全水平与风险程 度相一致，尤其包括如下内容： • 个人数据的**假名化**机制和**加密**措施；	网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。	• 个人信息控制者应根据有关国家标准的要求，建立适当的数据安全能力，落实必要的管理和技术措施，防止个人信息的泄漏、损毁、丢失。 • 个信息**存储时间最小**化； • 收集个信息后，宜立即进行**去标识化**处理，并采取技术和管理方面的	• **第五十条：**制定内部管理制度和操作规程； • **第五十条：**对个人信息实行分级分类管理； • **第五十条：**采取相应的加密、去标识化等安全技术措施； • **第五十条：**合理确定个人信息处理的操作权限，

• 确保处理系统和服务能够持续保持自身**保密性、完整性、有效性**和**自我修复**的能力； • 在物理性或技术性事故中**及时恢复**个人数据的有效性和对个人信息访问的能力； • 实施一项定期测试、评估、评价技术性和组织性措施**有效性**的程序以确保处理的**安全性**。		措施，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使 用的权限管理； • 对个人信息访问采取**控制措施**，如最小授权的访问措施策略、设置内部审批流程、角色权限分离； • 制定**应急预案**、定期组织**应急响应培训和演练**； • 设定个信息安全**负责机构和责任人**； • 在需求、设计、开发、测试、发布等**系统工程**阶段考虑个人信息保护要求，保证在系统建设时对个人信息保护措施同步规划、同步建设和同步使用。 • **人员管理与培训** • **安全审计**	并定期对从业人员进行安全教育和培训； • **第五十条：**制定并组织实施个人信息安全事件应急预案； • **第五十一条**（如适用）：指定个人信息保护负责人； • **第五十二条**（如适用）：设立境内专门机构或指定代表； • **第五十三条**：进行安全审计； • **第五十四条**：进行风险评估。 • **第五十六条**：发生个人信息泄露时的补救措施和通知报告义务。

9.2 对企业的合规提示

《网络安全法》中规定的“网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失，几乎在上述各法中都可查见，《民法典》的第一千零三十八条也有类似规定，实际上表达的就是要满足系统的安全（加密）、可控（分级分类），以达到保密性、完整性、有效性、可自我恢复。但《国标》和《个保法草案》都完整地提出了组织与流程上的管理要求。此外，从国家安全角度考虑，《数据安全法（草案）》第二十五条也要求企业开展数据活动，应当依照法律、行政法规的规定和国家标准的强制性要求，建立健全全流

程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。各法在总体思路上是一致的，但就如何做好上位法与下位法、法律与标准之间更好的衔接与调和，笔者提出如下基本建议：

第一，明确责任部门与人员。

- 明确法定代表人或主要负责人对个人信息安全负全面领导责任，包括为个人信息安全工作提供人力、财力、物力保障等；
- 满足条件的组织，应任命个人信息保护负责人和个人信息保护工作机构，个人信息保护负责人应由具有相关管理工作经历和个人信息保护专业知识的人员担任，参与有关个人信息处理活动的重要决策直接向组织主要负责人报告工作；
- 个人信息保护负责人和个人信息保护工作机构的职责应包括但不限于：
  - 全面统筹实施组织内部的个人信息安全工作，对个人信息安全负直接责任; 组织制定个人信息保护工作计划并督促落实;
  - 制定、签发、实施、定期更新个人信息保护政策和相关规程等。

第二，制定内部规章以确保各类数据保护措施能够得到有效实施。

- 建议企业制定数据安全管理政策等文件以确保数据安全保护措施能够得到有效的实施。

第三，对个人信息实行分级分类管理。

- **信息分级分类并实施特别保护措施**
- 建议企业根据所收集的个人信息具体情况区分个人敏感信息、儿童个人信息、金融数据等，并根据不同信息的要求实施特别保护措施：

  个人敏感信息的特别保护措施可参考《国标》等；

  儿童个人信息特别保护措施可参考《儿童网络个人信息保护规定》等；
- **履行等级保护要求**
- 建议企业应当依法开展网络定级备案、安全建设整改、等级测评和自查等工作，采取管理和技术措施，保障网络基础设施安全、网络运行安全、数据安全和信息安全，有效应对网络安全事件，防范网络违法犯罪活动。

第四，采取相应的加密、去标识化等安全技术措施。

- 建议企业应根据有关国家网络安全标准的要求，如有需要实时更新必要的管理和技术措施，防止个人信息的泄漏、损毁、丢失。加密、去标识化等

技术要求可参考相关的国家标准，包括《信息安全技术保护轮廓和安全目标的产生指南》（GB/Z 20283-2006）、信息安全技术网络安全等级保护安全管理中心技术要求》（GB/T36958-2018）等。

第五，合理确定个人信息处理操作权限，定期对从业人员进行安全教育和培训

- **建立个人信息的访问控制措施**
  - 建议公司对被授权访问个人信息的研发部门和运营部门的人员建立最小授权的访问控制策略，使其只能访问职责所需的最少够用的个人信息，且仅具备完成职责所需的最少的数据操作权限；若确因工作需要，需要超出权限处理个人信息的，应经公司个人信息保护责任人或个人信息保护工作机构进行审批，并记录在册。
  - 建议公司对个人信息的批量修改、拷贝、下载等重要操作设置内部审批流程。
  - 建议公司对个人敏感信息的访问、修改等操作行为，宜在对角色权限控制的基础上，按照业务流程的需求触发操作授权。例如，当收到客户投诉，投诉处理人员才可访问。
- **建立相应文件及制度确保员工遵循数据安全保护的义务与责任**
  - 建议公司在必要时，如个人信息涉密等级高时签订额外的保密协议。在工作人员离岗时，签署调离后个人信息保密义务的承诺书，防范内部员工、管理员因工作原因非法持有、披露和使用个人信息。
  - 建议公司在录用对个人信息处理岗位的相关人员设定特殊的要求或程序，对大量接触个人敏感信息的人员进行背景审查。此外，建议公司设立专人负责定期对接触个人信息数据工作的工作人员进行全面、严格的安全审查、意识考核和技能考核。
  - 建议公司明确内部涉及个人信息处理不同岗位的安全职责，建立发生安全事件的处罚机制。
- **定期对于员工进行数据安全培训**

  建议公司制定培训计划并定期（至少每年一次）按计划对各岗位员工进行基本的安全意识教育培训和岗位技能培训；制定安全教育和培训计划文档，明确培训方式、培训对象、培训内容、培训时间和地点等，培训内容包含信息安全基础知识、岗位操作规程等，并形成培训、教育记录。

第六，制定并组织实施个人信息安全事件应急预案

- **安全事件应急预案及提前准备**
  - 应制定个人信息安全事件应急预案，并根据法律法规要求变化及时更新元;
  - 应定期(至少每年一次)组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程;
- **安全事件处置**
  - 发生个人信息安全事件后，个人信息控制者应根据应急响应预案进行处置，包括记录事件内容、评估影响、采取必要措施、按照《国家网络安全事件应急预案》等有关规定及时上报等。
  - 如事件会对个人信息主体合法权益造成严重危害的，应按照要求向个人信息主体告知；若难以告知，应采取合理有效方式向公众发布警示信息。

第七，定期进行数据安全审计：

- 应对个人信息保护政策、相关规程和安全措施的有效性进行审计;
- 应建立自动化审计系统，监测记录个人信息处理活动;
- 审计过程形成的记录应能对安全事件的处置、应急响应和事后调查提供支撑;
- 应防止非授权访问、篡改或删除审计记录;
- 应及时处理审计过程中发现的个人信息违规使用、滥用等情况;
- 审计记录和留存时间应符合法律法规的要求。

10 个人信息控制者/个人信息处理者的义务

10.1 法规比标

GDPR	《网络安全法》	《国标》	《个保法草案》
考虑到处理行为的性质、范围、环境、目的以及可能对自然人的权利和自 由带来的	• 建立健全用户信息保护制度;	• 明确责任部门与人员; • 个人信息安全工程;	• **第五十条：**制定内部管理制度和操作规程; • **第五十条：**对个人信息实行分级分类管理;

风险和损害，数据控制者应当采取适当的技术和组织措施以确保并证明 处理行为是按照本法的规定进行的。这些措施应当在必要的情况下进行评估和更新。	• 不得泄露、篡改、毁损其收集的个人信息； • 未经被收集者同意，不得向他人提供个人信息（经过处理无法识别特定个人且不能复原的除外）； • 不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息； • 其他网络运营者应当履行的义务（例如网络安全等级保护等）。	• 个人信息处理活动记录； • 开展个人信息安全影响评估； • 具备数据安全能力； • 要对企业人员进行管理与培训； • 进行安全审计。	• **第五十条：**采取相应的加密、去标识化等安全技术措施； • **第五十条：**合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训； • **第五十条：**制定并组织实施个人信息安全事件应急预案； • **第五十一条：**（如适用）指定个人信息保护负责人； • **第五十二条：**（如适用）设立境内专门机构或指定代表； • **第五十三条**：进行安全审计； • **第五十四条**：进行风险评估。 • **第五十六条**：发生个人信息泄露时的补救措施和通知报告义务。

10.2 合规提示

《国标》上只有个人信息控制者这个概念，而 GDPR 中既有数据控制者又有数据处理者的概念。原来业界一直呼吁我国也可以像 GDPR 一样在控制者概念外，增加处理者的概念，以达到国际统一的表达方法和话语体系。但此次《个保法草案》却将原本《国标中》个人信息控制者的概念重新定义为了“个人信息处理者”，实则会给企业带来一些额外的困惑和解释成本，特别是那些本来就只履行处理者义务的企业（比如说云服务企业），其面对《个保法草案》第五章（个人信息处理者的义务）时究竟是不是需要全部或者部分履行这些义务呢就会非常不清晰。虽然《国标》只提出了控制者没有处理者的概念，但是对两者的义务还是比较清晰的，并且从《国标》实施前后企业也做了一定的实践工作，特别是控制者与处理者签署的 DPA（数据处理协议），一旦《个保法草案》将称谓替换后，不但会要求承担如修

订所有合同等大量工作，同时合同中双方义务可能由于名称的变化而发生混淆。关于个人信息控制者与处理者的实践指引，笔者将放于第二部分详细论述。

11 需要进行个人信息安全影响评估（PIA）的场景和义务

11.1 法规比标

GDPR	《网络安全法》	《国标》	《个保法草案》
当一种数据处理方式，尤其是采用新技术的，数据控制者应于处理前针对该处理对个人数据保护的影响进行评估。单一评估也可针对一系列呈现相似高风险操作进行评估 实施数据保护影响评估时，应寻求数据保护官意见。 特别适用情形如下： • 自然人系统性的及深入的个人特质评估，而该评估是基于自动处理（包括画像），且该评估的决定将对该自然人产生法律影响或其他类似重大影响。 • 大规模处理特殊类型的个人数据或刑事定罪和违法犯罪的个人数据；	/	建立个人信息安全影响评估制度，评估并处置个人信息处理活动存在的安全风险。 个人信息安全影响评估应主要评估处理活动遵循个人信息安全基本原则的情况，以及个人信息处理活动对个人信息主体合法权益的影响，内容包括但不限于： • 个人信息收集环节是否遵循目的明确、选择同意、最少必要等原则； • 个人信息处理是否可能对个人信息主体合法权益造成不利影响，包括是否会危害人身和财产安全、损害个人名誉和身心健康、导致歧视性待遇等； • 个人信息安全措施的有效性； • 匿名化或去标识化处理后的数据集重新识别出个人信息主体的风险； • 共享、转让、公开披露个人信息对个人信息主	第五十四条：个人信息处理者应当对下列个人信息处理活动在事前进行风险评估,并对处理情况进行记录 • 处理敏感个人信息； • 利用个人信息进行自动化决策； • 委托处理个人信息、向第三方提供个人信息、公开个人信息； • 向境外提供个人信息； • 其他对个人有重大影响的个人信息处理活动。 风险评估的内容应当包括： （一）个人信息的处理目的、处理方式等是否合法、正当、必要； （二）对个人的影响及风险程度；

对公众可访问区域的大规模系统性监控。		体合法权益可能产生的不利影响； • 如发生安全事件，对个人信息主体合法权益可能产生的不利影响。 产品或服务发布前，或业务功能发生重大变化时，应进行个人信息安全影响评估。 在法律法规有新的要求时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大个人信息安全事件时，应重新进行个人信息安全影响评估。 形成个人信息安全影响评估报告，并以此采取保护个人信息主体的措施，使风险降低到可接受的水平； 妥善留存个人信息安全影响评估报告，确保可供相关方查阅，并以适宜的形式对外公开。	（三）所采取的安全保护措施是否合法、有效并与风险程度相适应。 风险评估报告和处理情况记录应当至少保存三年。

11.2 合规提示

GDPR 中所涉及的 DPIA 主要有 29 条工作组制订的指南进行详细规定。主要有九类高风险行为会触发履行 DPIA 的义务：评估或评分、自动化决策产生法律或类似显著效果、系统性监控、敏感数据或高度个人性质的数据、大规模处理数据、匹配或者组合的数据集、易受攻击的数据主体的数据、创新使用或者应用新技术或者企业解决方案、处理本身阻止数据主体行使权利或者使用服务或合同。

《个保法草案》对个人信息安全影响评估制度做了概述性的规定，描述了需要进行 PIA 评估的情形，而《国标》则具体规定了需要进行安全影响评估的条件以及安全影响评估的具体内容。目前《个人信息安全影响评估指南》可提供更为具体的方法论和指引，尽管还在征求意见稿阶段，但企业可参考进行准备。

12 个人信息出境的要求

12.1 法规比标

GDPR	《网络安全法》	《国标》	《个保法草案》
在欧盟委员会没有作出认定决定时，数据控制者、数据处理者可向第三国或国际组织传输个人数据，当且仅当数据控制者、数据处理者提供了合适的保护措施，同时数据主体的权利能有效行使，其同时享有有效的法律救济途径。 • 合适的、不需要监管机构特定授权的保护措施包括以下： • 公权力部门之间签署的具有法律效力、能有效执行的法律文件 • 根据 47 条作出的有约束力的公司准则 • 欧盟委员会采用的标准数据保护条款 • 监管机构采用的、经欧盟委员会许可的标准数据保护条款	关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。 **《数据出境安全评估办法（征求意见稿）》** 网络运营者向境外提供其收集和产生的个人信息，应向个人说明数据出境的目的、范围、类型，以及接收方所在的国家或地区，并经其同意。为了保障公民生命和重大财产安全等紧急情况的除外。 拨打国际及漫游电话、发送国际电子邮件、进行国际即时通信、进行跨境交易以及其他个人主动行为，视为已经个人同意。	在中华人民共和国境内运营中收集和产生的个人信息向境外提供的，个人信息控制者应当遵循国家相关规定和相关标准的要求。	第三十八条：个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当至少具备下列一项条件： • 依照本法第四十条的规定通过国家网信部门组织的安全**评估**； • 按照国家网信部门的规定经专业机构进行个人信息保护**认证**； • 与境外接收方**订立合同**，约定双方的权利和义务，并监督其个人信息处理活动达到本法规定的个人信息保护标准； • 法律、行政法规或者国家网信部门规定的其他条件。 第三十九条：个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的身份、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式等事项，并取得个人的**单独同意**。

• 除根据第 40 条制定的、经许可的行为准则外，同时第三国的数据控制者或数据处理者还应作出具有约束力、可执行的承诺，采用合适的保护措施，包括保护数据主体权利的措施。 • 除根据第 42 条经过认证的机制外，同时第三国的数据控制者或数据处理者还应作出具有约束力、可执行的承诺，采用合适的保护措施，包括保护数据主体权利的措施。	**《个人信息出境安全评估办法（征求意见稿）》** 网络运营者向境外提供在中华人民共和国境内运营中收集的个人信息（以下称个人信息出境），应当按照进行安全评估。经安全评估认定个人信息出境可能影响国家安全、损害公共利益，或者难以有效保障个人信息安全的，不得出境。		**第四十条**：关键信息基础设施运营者和处理个人信息达到**国家网信部门规定数量**的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。 **第四十一条**：因国际司法协助或者行政执法协助，需要向中华人民共和国境外提供个人信息的，应当依法申请有关主管部门批准。中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息有规定的，从其规定。

12.2 合规提示

GDPR 对于跨境数据传输的机制进行了专章规定，主要包括四种数据出境机制：充分性决定、BCR、标准性条款和已经批准的行为准则。目前，企业用得较多的是标准性条款的路径（但也需要注意在 Schrems II 案件 后 SCC 也可能会被更新）。由于跨境传输本身是一个处理动作，除了上表所述的保护措施以外， 还需获得数据主体的同意或者满足其他合法事由所规定的情形。数据出境安全评估应重点衡量以下方面问题：

1）数据出境的合法性、正当性；

2）涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及是否

已经个人同意等；

3）涉及重要数据情况，包括重要数据的数量、范围、类型等；

4）网络运营者和数据接收方的安全保护能力、安全措施和环境等；

5）数据出境后再转移被泄露、毁损、篡改、滥用等风险；

6）其他可能严重影响个人信息和重要数据安全的风险。

《个保法草案》明确了跨境传输的前提条件。相较于此，2019 年出台的《个人信息出境安全评估办法（征求意见稿）》要求所有个人信息出境均应当进行安全评估和审查报批，此次《个保法草案》避免了一刀切式的要求，借鉴 GDPR 中关于 SCC、认证的相关规定，规定了网信办组织评估、专业机构进行个人信息保护认证、与境外接收方订立合同这三种情况，有利于促进数据在不同法域间的流通，也为企业数据进行正常商业贸易下的个人信息出境提供了更多选择和便利。但相较于此，GDPR 似乎给予企业更多选择，例如有约束力的公司规则（binding corporate rules）以及经过评估可以给予充分性保护（adequate level of protection）的国家等。

《个保法草案》第三十九条还要求企业对个人信息主体进行充分告知并征得个人信息主体的单独同意，这是否意味着在一揽子的隐私政策以外，如果触及个人信息出境，企业还需以弹窗等方式另行征得同意才能符合单独同意的要求吗，如果是，可能会给用户带来较不好的使用体验，也无疑可能增加企业的合规成本。因此，还有待个保法细则对“单独同意”的进一步解释。值得注意的是，《个保法草案》第四十条关于关键信息基础设施运营者的规定与《网络安全法》第三十七条规定基本一致，但同时增加了数据本地化的门槛，即个人信息达到一定数量的也需要境内存储。具体数量级可能有待于网信部门出台进一步的细则要求。关于个人信息出境的实践指引，笔者将放于本报告第二部分详细论述。

13 个人信息安全负责人的岗位和要求

13.1 法规比标

GDPR	《网络安全法》	《国标》	《个保法草案》
任命的门槛 在以下情形中，数据控制者和数据处理者应任命一名数据安全保护官 • 公权力机关处理个人数据的； • 核心数据处理活动，其范围、目的要求经常性、系统性、大范围地监测数据主体； • 核心数据处理活动，包括大规模处理特定类别的个人数据，或处理与刑事犯罪和起诉相关的个人数据。 注：“核心”是指完成组织目标的关键业务（包括个人数据处理是关键业务中不可或缺的情况，如医院）。 WP29 小组认为： • 风险治理的核心； • WP29 建议所有组织都任命 DPO，并认为 DPO 会是企业的核心竞争力； **定位** • DPO 具备法定定义，伴随着确定的权利和义务，企业不得随意使用该名称； • DPO 是联系各方（监管机构、数据主体、组织内部的各业务部门、媒体、社会监督组织等）的枢纽；	• 网络安全负责人：落实网络安全保护责任； • 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供； • 关键信息基础设施的运营者还应当设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查。	**任命的门槛** 应任命个人保护负责人和个人信息保护工作机构，个人信息保护负责人应 由具有相关管理工作经历和个人信息保护专业知识的人员担任，参与有关个人 信息处理活动的重要决策直接向组织主要负责人报告工作。满足以下条件之一的组织，应设立专职的个人信息保护负责人和个人信息保护工作机构，负责个人信息安全工作： • 主要业务涉及个人信息处理，且从业人员规模大于 200 人； • 处理超过 100 万人的个人信息，或在 12 个月内预计处理超过 100 万人的个人信息； • 处理超过 10 万人个人敏感信息。 **定位** 应为个人信息保护负责人和个人信息保护工作机构提供必要的资源，保障其独立履行职责。 **职责**	**第五十一条** **任命的门槛** 处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人。 **定位** 负责对个人信息处理活动以及采取的保护措施等进行监督。 **其他** 个人信息处理者应当公开个人信息保护负责人的姓名、联系方式等，并报送履行个人信息保护职责的部门。

• DPO 以合适的方式及时参与到涉及个人数据处理的所有事项中； • DPO 应具备履行职责所必需的资源，并具备资源保持其专业水准（如培训、参加会议等等）； • DPO 在行使职责时，不受控制者和处理者意见的影响，不得因其行使职责而对其开除或处罚； • DPO 直接向最高管理层汇报。 **职责** • 告知控制者、处理者，以及其雇员《条例》或其他欧盟或成员国法律所规定的义务，并提供建议； • 监测是否符合《条例》、其他欧盟或成员国法律、控制者或处理者数据保护政策的规定，包括内部的数据处理职责的分配、增强数据保护意识、培训、相关的审计等； • 对数据保护影响评估提出建议，并监控评估的开展； • 与监管机构合作； • 作为控制者或处理者对监管机构的联系人。 在考虑到处理的性质、范围、情境和目的后，数据保护官在行使其职责时应掌握数据处理的相关风险。		• 全面统筹实施组织内部的个人信息安全工作，对个人信息安全负直接责任； • 组织制定个人信息保护工作计划并督促落实； • 制定、签发、实施、定期更新隐私政策和相关规程； • 建立、维护和更新组织所持有的个人信息清单（包括个人信息的类型、数量、来源、接收方等）和授权访问策略； • 开展个人信息安全影响评估，提出个人信息保护的对策建议，敦促整改安全隐患； • 组织开展个人信息安全培训； • 在产品或服务上线发布前进行检测，避免未知的个人信息收集、使用、共享等处理行为； • 公布投诉、举报等信息并及时受理投诉举报； • 进行安全审计；	

注： • 合规事件发生后，控制者或处理者要承担责任，而非 DPO 本人； • 控制者或处理者如果对某一处理活动的意见与 DPO 不同，DPO 的意见应当被忠实地记录下来； • 类似于中纪委派驻各个组织的纪委书记。		• 与监督、管理部门保持沟通，通报或报告个人信息保护和事件处置等情况。	

13.2 合规提示

企业选任 DPO 的人选是非常关键的。GDPR 规定，是否具备相关法律知识、组织及技术知识和责任能力将成为被任命为 DPO 的首要因素。DPO 之职既可由内部员工担任，也可通过与外部人员签订“service contract”的方式担任。如何选择应取决于企业所涉及的数据量和预算。为独立性及持续性之目的，并根据 WP29 指南的建议，可与 DPO 建立至少 2 年的合作关系或者雇佣关系。企业应为 DPO 独立办公提供必要的资源，如 DPO 必须永远可以独立向最高管理者（层）进行汇报，且不因提出异议而被开除或者惩罚。一旦任命 DPO 便须立即公布其联系方式，并通过 DPO 与欧盟成员国监管机构沟通。尽管由 DPO 来履行协调、监管、审查的义务，但是责任承担的主体仍然是数据控制者或者处理者本身。

在我国，无论是《国标》和《个保法草案》中的个人信息保护负责人，在设立目的上和 DPO 存在相似性，当企业出现违法责任时，除对单位课以处罚外，如果个人信息保护负责人自身工作存在故意或过失或从事违法行为，因属于“直接负责的主管人员以及其他责任人员”，需要承担个人责任，包括民事、刑事和行政责任。

任命个人信息保护负责人是一项法定义务，因此，建议企业任命个人信息保护负责人和个人信息保护工作机构，个人信息保护负责人应由具有相关管理工作经历和个人信息保护专业知识的人员担任，参与有关个人信息处理活动的重要决策直接向公司主要负责人报告工作。个人信息保护负责人和个人信息保护工作机构的职责应包括但不限于：

1) 全面统筹实施组织内部的个人信息安全工作，对个人信息安全负直接责任；
2) 组织制定个人信息保护工作计划并督促落实；
3) 制定、签发、实施、定期更新隐私政策和相关规程；
4) 建立、维护和更新组织所持有的个人信息清单（包括个人信息的类型、数量、来源、接收方等）和授权访问策略；
5) 开展个人信息安全影响评估，提出个人信息保护的对策建议；
6) 组织开展个人信息安全培训；
7) 在产品或服务上线发布前进行检测，避免未知的个人信息收集、使用、共享等处理行为；
8) 公布投诉、举报方式等信息并及时受理投诉举报；
9) 进行安全审计。

由于《网络安全法》要求网络运营者依法设置网络安全负责人；《关键信息基础设施保护条例（征求意见稿）》要求关键信息基础设施的运营者还应当设置专门安全管理机构和安全管理负责人；《数据安全法（草案）》要求重要数据的处理者设立数据安全负责人；本次《个保法草案》要求个人信息处理者设立个人信息负责人。企业是否需要设立这么多的职位，这些职位是否需要专职，能否一人多岗等问题，笔者将于本报告第二部分详细论述。

14 个人信息安全事件的处理和报告要求

14.1 法规比标

GDPR	《网络安全法》	《国标》	《个保法草案》
在数据安全事故发生之后，数据控制方应当及时向监督机构报告，在可行时，应当在 **72 小时内**报告，除非数据安全事故不太可能导致数据主体权益受损。如未	网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网	• 应制定个人信息安全事件应急预案； • 应定期（至少每年一次）组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位	**第五十五条：**个人信息处理者发现个人信息泄露的，应当**立即**采取补救措施，并通知履行个人信息保护职责的部门和个人。

能在 72 小时内报告，应当提供合理的解释。 数据处理者在得知数据安全事故发生之后，应及时告知数据控制者。 告知应至少包含以下内容： • 如可能，应描述数据安全事故的性质，涉及的数据主体类别和大致人数，涉及的个人数据类别和大概数量 • 数据保护官的名字和联系方式，以及需更多信息的时可联系的人 • 描述数据安全事故可能带来的后果 • 描述数据控制者已经采取的、或将要采取的处置数据安全事故的措施，包括降低其不利影响的措施 如果无法同时提供所有的上述信息，则信息应及时、分阶段上报。 数据控制者应记录所有的数据安全事故，包括事故发生的事实、后果、补救措施。应将记录提供给监管机构，使其得以评估数据控制者是否遵守本条规定。	络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。	职责和应急处置策略和规程； • 发生个人信息安全事件后，个人信息控制者应根据应急响应预案进行以下处置： -记录事件内容，包括但不限于：发现事件的人员、时间、地点，涉及的个人信息及人数，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门； -评估事件可能造成的影响，并采取必要措施控制事态，消除隐患； -按《国家网络安全事件应急预案》的有关规定及时上报，报告内容包括但不限于：涉及个人信息主体的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式； -个人信息泄漏事件可能会给个人信息主体的合法权益造成严重危害的，如个人敏感信息的泄露，按照要求实施安全事件的告知。[1] • 根据相关法律法规变化情况，以及事件处置情况，及时更新应急预案。	通知应当包括下列事项： • 个人信息泄露的原因； • 泄露的个人信息种类和可能造成的危害； • 已采取的补救措施； • 个人可以采取的减轻危害的措施； • 个人信息处理者的联系方式。 个人信息处理者采取措施能够有效避免信息泄露造成损害的，个人信息处理者可以不通知个人；但是，履行个人信息保护职责的部门认为个人信息泄露可能对个人造成损害的，有权要求个人信息处理者通知个人。

14.2 合规提示

对于安全事故的处理，在安全事故发生时企业不仅要向用户告知，同时还要向监管机关作报告。GDPR 规定了数据泄露报告的时间要求：对数据主体的报告应该是 undue delay，对监管机构的报告需要不得晚于事故发生后的 72 小时内。报告内容需要涉及 1.所涉数据类型、数据主体数量；2.DPO 的姓名和联系方式；3.数据泄露可能造成的后果；4.将采取的处理措施。如果泄露未为数据主体造成风险，则可豁免报告义务（不建议企业以此为标准开展合规）。控制者须对泄露报告保留书面记录。但当控制者对个人数据施以适当的技术、组织保护措施（如加密），可以不通报数据主体，或者控制者已采取能够保证数据主体权利和自由不受高风险侵犯的措施。

《个保法草案》要求个人信息处理者发现个人信息泄露的，应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。这里的“立即”弹性较大，在满足《国家网络安全事件应急预案》中网络安全事件不同 level 不同要求情况下，有可能会比 72 小时相对宽松，但也有部门规章和地方性法规要求更短时间内，比如说《计算机信息系统安全保护条例》要求对计算机信息系统中发生的案件，有关使用单位应当在 24 小时内向当地县级以上人民政府公安机关报告。

《国标》还要求企业定期（至少每年一次）组织内部相关人员进行应急响应培训和应急演练，以防止真正发生事故时措手不及，不熟悉应急处置策略和规程。因此，建议企业根据我国《国家网络安全事件应急预案》以及《国标》中的规定，应事先准备完整妥善的应急预案并每年至少组织相关人员进行一次应急预案响应及应急培训。我国目前对发生安全事故时的预警机制和各个机构负责的义务已经规定的比较详细了，对于企业向有关机构报告的时间的规定，建议进行细化，这将有助于在第一时间控制事态发展， Facebook 在明知数据泄露给第三方且自己没有控制权的情况下，没有采取及时的补救措施，而是采取一种放任态度，如果他们能够及时的向社会公告、寻求政府部门的协助，那么最终也不会出现这么恶劣的局面。当然，也要根据企业实际情况，例如是否已经初步查明原因、是否已采取初步措施控制风险进一步恶化、是否了解清楚受影响人数、各部门是否已经应急准备就绪，来选择最佳时机上报和通知用户。

15 监管机构和罚则

15.1 法规比标

GDPR	《网络安全法》	《国标》	《个保法草案》
个案中考虑的因素： • 违规的性质、严重性及持续期间，并考虑到处理的性质范围或目的，以及受影响之数据主体人数及其受损程度； • 违规的故意或过失； • 所采减少数据主体损害的任何行为； • 控管者或处理者的责任程度，并考虑到其依第 25 条及第 32 条所实施的技术上及组织上的措施； • 违规所影响的个人资料类型； • 任何其他适用于该个案情形之加重或减轻因素，例如因违约而直接或间接获得的经济利益或避免的损失 。 **罚则** • 对于违反隐私保护设计，以及默认隐	网络运营者不履行相应的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，根据具体情况不同处以最低五千元最高一百万元（十倍违法所得）的罚款，并且还将有拘留、从业限制甚至刑法上的处罚。	尽管《国标》属于国家推荐标准，但在监管部门执法过程中已将其作为执法依据。	**第六十二条：**违反本法规定处理个人信息，或者处理个人信息未按照规定采取必要的安全保护措施的，由履行个人信息保护职责的部门责令改正，没收违法所得，给予警告；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 有前款规定的违法行为，情节严重的，由履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务、停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。 **第六十三条：**有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。 **第六十四条：**国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；对直接负责的主管人员和

私保护，没有实施充分的 IT 安全保障措施、违反数据泄露通知要求等等，处以 1000 万欧元或者上一年度全球营收的 2%，两者取其高； • 对于违反数据处理原则，数据处理没有合法基础，违法同意要求，侵害数据主体的合法权利等，处以 2000 万欧元或者企业上一年度全球营业收入的 4%，两者取其高。			其他直接责任人员依法给予处分。 **第六十五条：**因个人信息处理活动侵害个人信息权益的，按照个人因此受到的损失或者个人信息处理者因此获得的利益承担赔偿责任；个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，由人民法院根据实际情况确定赔偿数额。个人信息处理者能够证明自己没有过错的，可以减轻或者免除责任。 **第六十六条：**个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、履行个人信息保护职责的部门和国家网信部门确定的组织可以依法向人民法院提起诉讼。 **第六十七条：**违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

15.2 合规提示

GDPR 生效后，原来由各欧盟成员国数据保护机构（DPA）分别管辖本司法区域的模式已经转变为由独立的欧盟数据保护委员会（EDPB）进行统一监管，发表意见与提供指导，确保 GDPR 适用的一致性并向欧盟委员会作出报告。

在 GDPR 项下，当数据控制者或者处理者违反相关规定，未遵守数据处理的基本原则和合法事由的规定，对数据主体的权利造成损害时，数据主体有权直接向监管机构进行投诉，监管机构可决定向其提供司法救济渠道，以及是否对违规主体进行行政处罚。GDPR 规定了严厉的处罚机制，企业应当评判自身的风险点，从高风险点合规入手，避免带来现实的法律风险。对于大企业、处理大量数据的企业，其

合规要求较高，其面临法律风险的几率也会增大。另外，如果企业遭受消费者投诉或者发生了数据泄露事件，那就必然会引起监管机构的调查，因此需要谨慎对待，避免遭受高额罚款。当然，GDPR 也允许在事件发生后，企业通过积极避损的方式来减轻处罚数额。

由于《国标》是推荐性的国家标准，因此违反网络安全保护义务的罚则规定在网络安全法中，网络运营者需要承担相应的行政、民事与刑事责任。此次《个保法草案》较为引发关注的一点是其严格和高昂的违法成本，最高可达到五千万元以下或上年度营业额百分之五以下的罚款。值得注意的是，《个保法草案》并没有严格界定什么情况属于“情节严重”，但结合 GDPR 相关处罚案例来说，数据泄露、受影响的信息主体数量可能成为较大的考虑因素。同时《个保法草案》第六十二条使用了“拒不改正”这样的表达，因此笔者认为无论在何种情况下，展现出积极的改正态度始终是优解。

笔者还注意到，《个保法草案》第六十六条明确了个人信息公益诉讼的可行性。根据《民事诉讼法》第五十五条，对损害社会公共利益的行为，法律规定的机关和有关组织可以向人民法院提起诉讼。法律规定的机关和有关组织不提起诉讼的情况下，人民检察院可以向人民法院提起诉讼。法律规定的机关和有关组织提起诉讼，人民检察院也可以支持起诉。《个保法草案》此次明确将违法处理个人信息侵害众多个人权益的情况纳入公益诉讼范畴。这也正是此次《个保法草案》较有特色的地方，将公法与私法救济进行融合。

特别地，《个保法草案》第九条规定“个人信息处理者应当对其个人信息处理活动负责”，尽管不像 GDPR 第 5 条 5 款那样明确要求数据控制者“应能够证明”其遵守了数据处理原则，没有明确规定“自证合规”要求，但该草案在第六十五条规定了“个人信息处理者能够证明自己没有过错的，可以减轻或者免除责任”，即“不能证明自己没有过错的就应对数据处理活动导致的损害后果承担赔偿责任”，从而通过“法律”规定了个人信息处理者在承担民事赔偿责任时的过错推定原则，呼应了《民法典》（侵权责任编）第 1165 条 2 款中规定[1]，只有依照“法律规定”才能适用过错推定原则承担侵权责任的要求，同时也与 GDPR 第 82 条 3 款的规定“类似”（数据控制者和处

[1] 《民法典》第 1165 条第 2 款：行为人因过错侵害他人民事权益造成损害的，应当承担侵权责任。依照法律规定推定行为

理者证明其对产生损害的事件负任何责任的，免于承担损害赔偿责任）。因此，企业必须在日常经营过程中，做好记录和存证义务。例如庞先生诉东航、去哪儿一案，当原告（个人信息主体）无法且无能力举证证明被告（企业）存在侵害公民个人信息行为时，企业负有举证责任倒置义务，即需要向监管机构展示和解释其处理行为是合规的。另一方面，如果个人信息处理者（此处指《个保法草案》下的术语）需要承担《个保法草案》中未涉及的其他民事责任形式（特别是侵犯人格权时一般适用的消除影响、恢复名誉、赔礼道歉等责任形式），笔者理解也应该遵从“过错推定”原则，但当企业被实施行政处罚时，其应直接适用《行政处罚法》等公法领域的责任规定，不应再适用过错推定原则。因个人信息保护法领域兼具公私法交织的特点，其归责原则也比较多元，在适用时还需要更多司法案例进行验证和澄清。

16 结语

《个保法草案》是我国个人信息保护立法进程中所跨的重要一步，但依然有不少待决问题。例如，GDPR 明确区分了控制者和处理者的概念，而《个保法草案》对于个人信息处理者的界定实际上与 GDPR 所规定的控制者是同一内涵。尽管这在理论上属于不同的解释选择问题，但在全球化数据合规的大背景下，可能会带来一些额外的解释成本。

此外，《个保法草案》中的定义可能会带来一些歧义，例如第二十一、二十二、二十三条分别规定了“共同处理”、“委托处理”、 “因合并、分立等原因转移个人信息”的情形，而第二十四条又提及了“向第三方提供”，那么第二十四条是否将第二十一、二十二、二十三条所述的情况均包含在内，可能需要进一步考虑。结合前述比标项中，需要个法保正式稿或者相关细则进一步解读的内容，在附录中进行了归总。

《个保法草案》的公布标志着我国在个人信息保护方面的一大步，尽管《个保法草案》目前正处于征求意见稿阶段，但依然体现了目前国家对于个人信息保护的监管趋势，同时鉴于《个保法草案》所规定的高昂违法成本，建议企业尽早进行自查，注重进行安全影响评估、制定内部管理制度、对个人信息进行分级分类和加密存储等安全措施、确定内部操作权限、记录处理活动、制定应急预案、定期进行审

人有过错，其不能证明自己没有过错的，应当承担侵权责任。

计和培训演练，发挥内部能动性和外部机构优势，定制一套综合全面、可持续、能落地的数据合规体系。除前述共通的比标项外，针对《个保法草案》的其他内容，笔者进行了逐条评论，请详见附录。

最后，还需要企业提前做好《网络安全法》、《民法典》、《个保法草案》、《数据安全法（草案）》以及《国标》中所有与个人信息保护相关的立法要求的衔接适用与统一落地措施的执行，以避免重复合规成本或高额罚款的发生。真正做到企业数据有效流动而增大经济效益同时，尊重用户隐私期待并保护好个人信息主体的信息安全。

17 附录 1

需要通过个保法正式稿或者细则进一步澄清或者解释的内容：

《个保法草案》条款	具体需澄清的内容	在报告中的页码
第三条	境外个人信息处理者在境内代表具体由谁来担任。	9
第十三条	同意与其他事由的选择与平衡。	17
第十四条—第十七条	未来企业是否需要为不同的处理活动确定不同的法律依据，以及企业是否可以在论证和选择法律依据。	20
第二十四条	此处“提供”是否包含《草案》第二十一、二十二、二十三条的情形，还是仅针对其中一种情形。	53-54/57
第三十七条	被评估的国家机构本身不应作为评估出境决定的机关本身。	59
第四十条	个人信息达到一定数量的也需要境内存储。	43
第四十二条	类似“黑名单”的限制清单如何做到日常监管与更新。	9
第四十四条	拒绝处理个人数据的平衡。	30
第四十八条、第四十九条	企业进行解释的合规方法以及与成本的平衡。	30
第二十五条	除了自化决策以外，是否对于基于一般画像的决策以及个性化展示/推送的规定。	31
第七章	处罚的影响因素。	7
“单独同意”（第二十四条、第二十六条、第二十七条、第三十条、第三十九条）与“书面同意”（第十四条、第三十条）	如何分别满足“单独同意”或“书面同意”的要求，以及这两者是否就一定是等效。	21
第六十九条	自动化决策的定义没有体现出自动化决策是一种不存在“人为干预性”的特点。	62

18 附录 2

本报告比标分析部分未提到的《个保法草案》其他条款，简要解读如下：

《个保法草案》	环球评论
第一章 总则	
第十一条 国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关行业组织、社会公众共同参与个人信息保护的良好环境。	未来个人信息将成为国家监管重点。特别是近年来，国家高度重视数据在新常态中推动国家现代化建设的基础性、战略性作用中共中央、国务院《关于构建更加完善的要素市场化配置体制机制的意见》： ➢ 将**数据**列为与土地、劳动力、资本、技术平行的五大要素领域； ➢ 明确要求制定数据隐私保护制度和安全审查制度。 除了加强国内的个人信息保护以及治理外，国家也会积极参与国际层面对个人信息这一蓝海领域的规则制定与国际合作，推动个人信息保护标准的国际互认。
第十二条 国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等的互认。	
第二章 个人信息处理规则 **第一节 一般规定**	
第十八条 个人信息处理者在处理个人信息前,应当以显著方式、清晰易懂的语言向个人告知下列事项： (一) 个人信息处理者的身份和联系方式； (二) 个人信息的处理目的、处理方式，处理的个人信息种类、保存期限； (三) 个人行使本法规定权利的方式和程序； (四) 法律、行政法规规定应当告知的其他事项。 前款规定事项发生变更的,应当将变更部分告知个人。	针对向个人信息主体的告知义务，《个保法草案》与《国标》基本一致，从颗粒度上而言《国标》更为细致，除了上述的内容外，要需要告知对外共享、转让、公开披露的情况；提供个人信息后可能存在的安全风险，及不提供个人信息可能产生的影响；遵循的个人信息安全基本原则等。 此外，如果 App 开发者，还需要进一步遵守与 App 相关的特定要求，例如《网络安全标准 2020 自评估指南—移动互联网应用程序（App）收集使用个人信息自评估指南》、《App

个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。	违法违规收集使用个人信息行为认定方法》、《网络安全标准实践指南—移动互联网应用程序（App）个人信息保护常见问题及处置指南》、《 网络安全标准实践指南– 移动互联网应用程序个人信息安全防范指引》等。
第十九条 个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条规定的事项。 紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后予以告知。	此条规定了需要告知个信息主体的例外情况：即基于法律法规规定需要严格保密，以及基于紧急情况（为保护自然人的生命健康和财产安全）当时无法告知的。
第二十条 个人信息的保存期限应当为实现处理目的所必要的最短时间。法律、行政法规对个人信息的保存期限另有规定的，从其规定。	明确个人信息的存储时间应当最小化，具体各类是个人信息的存储时间需要结合处理目的进行个案判断以及参考特别法规对存储期限的规定。《个保法草案》本身没有对超期存储的个人信息应当作何种处理进行规定，但可以参考《国标》进行删除或匿名化。
第二十一条 两个或者两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是，该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。 个人信息处理者共同处理个人信息，侵害个人信息权益的，依法承担连带责任。	虽然《个保法草案》没有像 GDPR 一样提出“共同控制者”的概念，但明确了共同决定个人信息处理目的和处理方式的，应当约定各自的权利和义务。因此，为明晰双方责任边界，建议签署数据处理协议。并且，进一步明确，即使数据处理者之间有合同约定，但不影响任何一个个人信息处理者对外承担连带责任，对内可根据约定分担责任。
第二十二条 个人信息处理者委托处理个人信息的，应当与受托方约定委托处理的目的、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托方的个人信息处理活动进行监督。 受托方应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息，并应当在	与《国标》中关于委托处理的规定基本一致。

合同履行完毕或者委托关系解除后，将个人信息返还个人信息处理者或者予以删除。 未经个人信息处理者同意，受托方不得转委托他人处理个人信息。	
第二十三条 个人信息处理者因合并、分立等原因需要转移个人信息的，应当向个人告知接收方的身份、联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新向个人告知并取得其同意。	与《国标》中关于收购兼并时转让个人信息的规定基本一致。
第二十四条 个人信息处理者向第三方提供其处理的个人信息的，应当向个人告知第三方的身份、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收个人信息的第三方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。第三方变更原先的处理目的、处理方式的，应当依照本法规定重新向个人告知并取得其同意。 个人信息处理者向第三方提供匿名化信息的,第三方不得利用技术等手段重新识别个人身份。	此处“提供”是指委托处理或者共享或者两类情况兼具或者其他情形，《个保法草案》没有给出明确答案，有待于正式稿的解答。但根据《侵犯个人信息罪司法解释》第三条规定，“提供公民个人信息”的行为有：一，向特定人提供公民个人信息；二，通过信息网络或者其他途径发布公民个人信息；三，未经被收集者同意，将合法收集的公民个人信息提供给他人（经过处理无法识别特定个人且不能复原的除外）。
第二十七条 在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、个人身份特征信息只能用于维护公共安全的目的，不得公开或者向他人提供；取得个人单独同意或者法律、行政法规另有规定的除外。	在《国标》2020 版本中对个人生物识别信息的规定以外，进一步回应了公共场所收集人脸信息如何获得用户同意的实践难题。但同时进行了更严格的规定，即仅可用于公共安全目的，并需要设置显著的提示标识。关于人脸信息、身份识别设备的更细致规定有待于未来更加细致的解答。本报告第二部分也会对人脸信息的收集使用进行深入分析建议。
第二十八条 个人信息处理者处理已公开的个人信息，应当符合该个人信息被公开时的用途；超出与	对于已公开的个人信息也作出了相关保护，只有符合个人信息主体授权公开的处理目的范围内才能进行处理。本条对于使用爬虫技术爬取平台上公开个人信息（如昵称、头像、性别

该用途相关的合理范围的，应当依照本法规定向个人告知并取得其同意。 个人信息被公开时的用途不明确的，个人信息处理者应当合理、谨慎地处理已公开的个人信息；利用已公开的个人信息从事对个人有重大影响的活动，应当依照本法规定向个人告知并取得其同意。	等）泛滥的情况起到了一定的规制作用：爬取方不得将“公开”的用户个人信息视为个人信息主体未对使用目的有限而肆意爬取并进行营利。因此《个保法草案》要求爬取方，如果利用公开的个人信息从事对个人信息主体有重大影响活动的，应当告知信息主体相关目的并且取得同意。如果个人信息被公开时用途不明确的，需要谨慎处理或者不处理。这也是继《数据安全管理办法（征求意见稿）》对网络爬虫行为在流量上有限制要求以外，另外一条被爬方可以通过行政手段进行救济的法律条款。
第二章 个人信息处理规则 **第二节 敏感个人信息的处理规则**	
第三十一条 个人信息处理者处理敏感个人信息的，除本法第十八条规定的事项外，还应当向个人告知处理敏感个人信息的必要性以及对个人的影响。	《国标》规定收集使用敏感个人信息的，需要在个人信息保护政策中明确标识或突出显示。此次《个保法草案》要求向信息主体告知处理敏感信息的必要性和影响。
第三十二条 法律、行政法规规定处理敏感个人信息应当取得相关行政许可或者作出更严格限制的，从其规定。	未来相关法律法规可能对敏感个人信息做出更严格的规定，《个保法草案》对此预留了空间。
第二章 个人信息处理规则 **第三节 国家机关处理个人信息的特别规定**	
第三十三条 国家机关处理个人信息的活动适用本法；本节有特别规定的，适用本节规定。	《个保法草案》新增国家机关处理个人信息时应当履行的义务，以更好地对个人信息保护起到监督审查作用。
第三十四条 国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。	国家机关也需要依法依程序操作，不得超出法定职责和必要范围处理公民个人信息。
第三十五条 国家机关为履行法定职责处理个人信息，应当依照本法规定向个人告知并取得其同意；	除有法律法规规定应当保密或者取得同意会妨碍其履行法定职责的（例如公安机关侦查逃犯

法律、行政法规规定应当保密，或者告知、取得同意将妨碍国家机关履行法定职责的除外。	等），国家机关处理个人信息也需要依法依程序操作，应当向信息主体进行告知并取得同意。
第三十六条 国家机关不得公开或者向他人提供其处理的个人信息，法律、行政法规另有规定或者取得个人同意的除外。	国家机关也与私营主体一样，不得随意公开或向第三方提供公民的个人信息，法律法规另有规定或者取得个人同意的除外。
第三十七条 国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行风险评估。风险评估可以要求有关部门提供支持与协助。	此条与《网络安全法》第 37 条对关键信息基础设施运营者的规定比较类似，国家机关处理的个人信息原则上应当在境内存储。针对确需向境外提供的，可能需要与《网络安全法》第 37 条有所区分，对于被评估的国家机构本身不应作为评估出境决定的机关本身，但当前的《个保法草案》没有过多涉猎，期待正式稿可以有所考虑。
第三章 个人信息跨境提供的规则	
第四十一条 因国际司法协助或者行政执法协助，需要向中华人民共和国境外提供个人信息的，应当依法申请有关主管部门批准。 中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息有规定的，从其规定。	此处是介绍国际司法协助需向境外提供个人信息，需履行报批义务，此要求在《数据安全法草案》中也有体现。《草案》第三十三条规定，境外执法机构要求调取存储在中华人民共和国境内数据的，有关组织、个人应当向有关主管机关报告，获得批准后方可提供。即企业在面临境外监管机构的直接执法时，不能径直提供境外监管机构要求的数据，而是需要先行上报给我国主管机关，获得批准后方才可提供。
第四十三条 任何国家和地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者该地区采取相应措施。	随着我国科技企业的兴起和 5G 等尖端技术的开发，各国针对我国企业的限制性措施层出不穷。例如，美国联邦通信委员会（FCC）将中国两大电信巨头企业列为国家安全威胁名单；印度电子信息技术部以“有损印度主权、国防、国家安全和公共秩序”为由宣布禁用 TikTok、微信等 59 款中国应用。本次《个保法草案》针对任何国家和地区对我国个人信息方面保护方面有歧视性的禁止、限制或者其他类似措施的，提出反制措施，可视为对近期国内企业在

	海外所面临的执法困境提供了国内法支持。此要求在《数据安全法草案》中也有体现。《数据安全法草案》第二十四条表明我国面对任何国家或地区对数据及对其开发利用技术相关的投资、贸易领域存在歧视的，我国将根据实际情况对该国家或者地区采取相应的措施。
第六章 履行个人信息保护职责的部门	
第五十六条 国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。 县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。 前两款规定的部门统称为履行个人信息保护职责的部门。	本次《个保法草案》通过法律层面设立专章的方式，规定了履行个人信息保护职责的部门的相关权利、职责与可能采取的相关措施，这也是比较大的亮点。 履行个人信息保护职责的部门主要包括国家网信办以及其他国务院有关部门和县级以上地方人民政府，可对个人信息处理活动进行约谈、询问、查阅、现场检查、查封或扣押等，并可接受投诉和举报。
第五十七条 履行个人信息保护职责的部门履行下列个人信息保护职责： (一) 开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作; (二) 接受、处理与个人信息保护有关的投诉、举报； (三) 调查、处理违法个人信息处理活动； (四) 法律、行政法规规定的其他职责。	
第五十八条 国家网信部门和国务院有关部门按照职责权限组织制定个人信息保护相关规则、标准，推进个人信息保护社会化服务体系建设,支持有关机构开展个人信息保护评估、认证服务。	
第五十九条 履行个人信息保护职责的部门履行个人信息保护职责，可以采取下列措施：	

(一) 询问有关当事人,调查与个人信息处理活动有关的情况； (二) 查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料； (三)实施现场检查,对涉嫌违法个人信息处理活动进行调查； (四)检查与个人信息处理活动有关的设备、物品；对有证据证明是违法个人信息处理活动的设备、物品,可以查封或者扣押。 履行个人信息保护职责的部门依法履行职责,当事人应当予以协助、配合，不得拒绝、阻挠。	
第六十条 履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈。个人信息处理者应当按照要求采取措施,进行整改,消除隐患。	
第六十一条 任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。 履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。	
第七章 法律责任	
第六十四条 国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。	与《国标》规定适用于各类组织、主管监管部门、第三方 评估机构相同，《个保法草案》从法律层面上要求国家机关如同私营主体，在没有遵守《个保法草案》或其他个人信息保护法律法规时，不无例外地面临相关行政处罚。
第八章 附 则	

第六十八条 自然人因个人或者家庭事务而处理个人信息的，不适用本法。 法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的，适用其规定。	《个保法草案》不适用于个人家庭事务、政府统计、档案管理中的个人信息处理活动。
第六十九条 本法下列用语的含义： （一）个人信息处理者，是指自主决定处理目的、处理方式等个人信息处理事项的组织、个人。 （二）自动化决策，是指利用个人信息对个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，通过计算机程序自动分析、评估并进行决策的活动。 （三）去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。 （四）匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。	• 《个保法草案》与《国标》就使用对象采用了不同的规范术语。根据对应术语的含义，《个保法草案》采用的术语为“个人信息处理者”，而《国标》采用的是“个人信息控制者”。笔者理解《个保法草案》之所以采用此术语是为了与《民法典》中的术语对齐，但可能与国际层面个人信息立法采用的“控制者”与“处理者”二分的形式可能会产生理解上的混淆。 • 自动化决策的定义没有体现出自动化决策是一种不存在“人为干预性”的特点，期待正式稿有更加精准的表达。 • 《个保法草案》“去标识化”的定义与《国标》相比，没有写入通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法“关联”个人信息主体的过程，这也正好印证本报告前述分析《个保法草案》对个人信息认定只作“识别”不作“关联”的要求。 • 《个保法草案》“匿名化”的定义与“去标识化”的情况相同，也只有提到“识别”没有“关联”要求。另外，《国标》还进一步规定了，个人信息经匿名化处理后所得的信息不属于个人信息。这为企业对匿名化后的信息不属于个人信息起到更加直接的判断帮助。

第二部分： 5 项具体个人信息保护要求深入分析

第一篇：关于敏感个人信息（人脸信息）的合规治理要求

在全球范围内，各国已经对个人信息及隐私保护意识有所提高，并逐步建立起本国的数据保护法律体系。不同敏感度程度的个人信息往往需要采取不同的规制方式，敏感程度越高的个人信息，往往会被予以特别关注。普遍来看，大多数国家针对需特殊关注的个人信息采取了单独定义的方式，同时，也针对此类数据的处理活动提出了特殊规范。例如有些国家可能使用“敏感个人信息”的概念，有些可能使用“特别种类（special category）的个人信息”，有些可能没有明确“敏感个人信息”的定义，却将相关的数据保护包括在生物识别信息的范畴内。尽管相关术语称谓不同，但可以反映出立法对于这类个人信息的特殊关注。而其中，生物识别信息因其具有唯一性和较强识别性的特点，通常被特殊关注。

经过调研，笔者发现对于包括人脸在内的生物识别信息，各国在规制程度上呈现多样性。如本报告第一部分所述，欧盟 GDPR 作为全球在数据保护方面具有立法理念领先、影响力广泛的一部法律，不光对欧洲各国自行制定数据保护法律法规起到了指引作用，同时也影响着非洲、亚洲、南美洲等正处于数据保护立法萌芽状态的其他国家和地区。虽然 GDPR 将生物识别信息明确定义为“通过对自然人的物理、生物或行为特征进行特定的技术处理而获得的个人数据”[2]，并且“这类数据生成该自然人的唯一标识，比如人脸图像或指纹识别数据” [3]，但并没有对生物识别信息的数据处理等行为进行特殊的额外规定。这可能是为欧盟国家内部根据自身情况制定更为具体的生物识别信息的法律规范预留空间，但也难免导致因规范缺位，而使部分国家忽视了对包括人脸信息在内的生物识别信息处理行为的规制。

经过环球数据合规团队的初步调研，笔者发现目前对于生物识别信息已有明确的定义，且对该类数据处理活动进行了特殊规定的国家和地区主要有：中国大陆、中国香港、美国（如加州、伊利诺伊州、新罕布什尔州、德克萨斯州、华盛顿州等）、英国、俄罗斯、法国、德国、荷兰、波兰、意大利、比利时、匈牙利、

[2] GDPR，第 4 条第（14）款。

[3] GDPR，第 4 条第（14）款。

罗马尼亚、葡萄牙、南非、泰国以及乌兹别克斯坦等等。同时，还有如博茨瓦纳、牙买加、巴基斯坦等国家，虽然明文立法还未生效，但也已经在起草的或待审议的法律提案中提及了生物识别信息的概念，并计划对此类信息的数据处理活动进行特别规范。

尽管如此，全球大部分国家其实尚处于虽然划分了生物识别信息的定义，但却没有提出专门规定处理该信息行为的状态；小部分国家和地区还没有数据保护相关的法律法规，仅在如宪法、民法等成文法中提到公民享有隐私权或个人信息权益等近似的规定。值得注意的是，在当今技术迅速发展的时代，人工智能技术不断创新更迭，生物识别信息的收集、处理、存储等一系列数据处理活动愈发普遍，其中最为典型和突出的则是企业对人脸信息的利用。人脸识别技术近年来在国内外得到了广泛的应用，落地场景也日益增多，包括通过人脸进行登录、支付等，商业发展空间广阔。在我国，根据《国标》，生物识别信息包括个人基因、指纹、声纹、掌纹、虹膜、面部特征等。而《个保法草案》以专节的形式规定了敏感个人信息[4]，并将个人生物特征纳入敏感个人信息的保护范畴。此外，关于人脸识别、声纹、基因数据等国家标准也在制定过程中。

从技术中立的角度出发，人脸识别技术本身无好坏之分，但是该技术的不成熟和缺乏监管规则的局面可能会导致该技术被不当使用，从而给个人信息主体的隐私安全带来威胁。

因此，本文将以收集使用**人脸信息**应当注意的合规要点为视角和着力点，重点介绍并分析我国大陆境内外对于使用人脸识别技术问题的监管态度，希望能为企业合规处理人脸识别信息提供相关思路与启发。需要特别指出的是，由于有些国家将人脸纳入生物识别信息/敏感个人信息的规制范畴，而未单独就人脸信息进行规定，因此在行文过程中，不可避免将提到敏感个人信息/生物识别信息中的相关规定。

一、域外法对人脸信息的监管态度

从域外的立法实践来看，目前对于人脸识别技术进行专门立法的法域不多，各法域大多采取在一般的个人信息保护规范中对生物识别信息、生物识别符等加

[4] 《个保法草案》第二章第二节规定了“敏感个人信息的处理规则”，仅为保持术语统一性，本文将统一称为“敏感个人信息”。

以规范的方式，对人脸识别技术的合规要点进行提示，但也有对人脸技术和人脸信息进行特殊保护的法域，例如美国加利福尼亚州近期通过的人脸识别技术的专门法案（Assembly Bill No.2661，以下简称“《加州人脸识别技术法案》”）。下文将从使用人脸识别技术生命周期的角度，对域外法的监管态度进行简要梳理。

（一）相关定义

目前，较多法域认为，通过人脸识别技术获取的信息为“生物识别信息”（Biometric Data），属于“敏感个人信息”，应当按照敏感个人信息的要求进行规制。以印度 2019 年 12 月提交下议院（Lok Sabah）的《个人数据保护法（草案）》为例，“敏感个人信息”的定义中包括生物识别信息，而“生物识别信息”的定义中则涵盖了“面部图像（facial images）”[5]，因此按此逻辑推演，通过人脸识别技术获取的信息应当作为敏感个人信息进行规制。澳大利亚 1988 年《隐私法案》也采取了相似的方式。

值得注意的是，欧盟 GDPR 将面部图像（facial image）也定义为“生物识别信息”，并将其归入了“特殊种类信息”。

据环球数据合规团队调研，美国各州或城市在应对人脸识别技术发展的立法活动中表现积极，通过本辖区内的单行立法对利用此类信息的活动进行直接规制。例如加利福尼亚州《加州人脸识别技术法案》、伊利诺伊州《生物信息识别法案》（以下简称“BIPA”）、德克萨斯州《商法典》第 503 章规定“生物识别符”（Business and Commerce Code, TITLE 11. PERSONAL IDENTITY INFORMATION, SUBTITLE A. IDENTIFYING INFORMATION, CHAPTER 503. BIOMETRIC IDENTIFIERS）以及《华盛顿州修订法典》第 19.375 章规定“生物识别符”（Chapter 19.375 Revised Code of Washington (RCW)）等。

相较以上法域，日本与韩国对人脸识别技术获取信息的监管规则可能较少。日本在 2016 年大幅修改《个人信息保护法》（以下简称“AAPI”）并在 2020 年再次进行了修订，但并未明确对面部信息进行定义。韩国 2020 年 2 月新修订的《个人信息保护法》（以下简称“PIPA”）也未明确提及生物识别数据的条文，且 PIPA 定义的敏感个人信息未明确涵盖生物识别数据。特别地，PIPA 第 25 条对影像数据处理设备的使用作出规定，可能涉及人脸识别技术设备的设置问题，但是 PIPA

[5] 印度《个人数据保护法案》（2019），第一章第三条第（7）款。

总体上仍然对使用相关设备处理影像数据持严格限制的态度。从个人信息保护法角度，尽管日韩并没有明确的人脸识别信息的概念，但是根据日韩对于“个人信息”的定义，个人信息具有可识别性。基于此，笔者合理推测，在日本、韩国法项下，人脸信息也需要适用一般个人信息的保护规则。

（二）信息收集

关于企业能否收集人脸识别信息的问题，多数法域的立法保留了合法空间，但大多会要求企业清晰告知个人收集信息的目的，并明确征得个人数据主体的同意。具体而言，不同法域大致可分为以下几种情形：

1. 原则上不禁止，满足法定条件即可收集

以美国《加州人脸识别技术法案》第 1798.310(d)条为例，数据控制者在公共场所使用人脸识别技术，需要以显著且符合实际特定场景的方式向个人信息主体进行告知，告知内容包括但不限于：（1）人脸识别技术的使用目的；（2）其可获取的通知、条款或政策的网站链接；以及（3）如何行使其主体权利等。根据第 1798.310(e)条，控制者在将个人信息主体的人脸图像纳入在对公众开放的物理场所中使用的面部识别服务之前（安保或安全的目的除外），应获得个人的同意。

2. 原则上禁止，除非征得个人信息主体同意

美国伊利诺伊州 BIPA 要求企业对使用人脸识别技术的情况进行充分披露。例如，BIPA 第十五节要求以书面形式向个人信息主体告知企业正在收集或存储生物标识或生物识别信息以及收集、存储和使用生物标识符或生物识别信息的特定目的与期限，并且需收到个人信息主体的书面同意才可被认定为获得同意。

美国德克萨斯州《商法典》第 503.001（b）条规定，任何人不得出于商业目的而获取其生物标识符，除非：（1）在获取生物标识符之前通知信息主体；并且（2）收到信息主体的同意。

类似地，美国《华盛顿州修订法典》第 19.375 章“生物识别符”中规定，（1）未经事先提供通知、征得主体同意或提供登记后禁止将生物标识符用于商业目的的机制，任何人不得在进行商业目的服务的数据库中登记生物标识符。（2）通知是一种披露，不被视为信息主体的肯定性同意。通知需要通过合理程序以容易获取的方式提供给信息主体。通知和同意类型取决于因具体情况而异。

3. 原则上禁止，除非具有正当事由（包括个人信息主体同意）

澳大利亚《隐私法案》中第 3 项隐私保护原则规定，原则上企业（organization）[6]不得收集敏感个人信息，除非征得了个人信息主体同意，并且该信息对于组织的运营来说是必要的，或者收集该信息具有以下事由：（1）该信息为澳大利亚法律、法院或仲裁庭法令要求或授权获取；（2）出现通常被允许的与收集行为有关的情形；（3）出现被允许的与收集行为有关的健康问题；（4）该企业为非盈利机构，并且同时满足收集以下两个条件：收集的信息与企业运营活动相关、收集的信息只与该企业的成员相关或与该企业有惯常联系的人员相关。[7]

GDPR 第 9 条规定，原则上不得处理特殊种类的个人信息，除非具有以下事由：（1）个人信息主体明示同意；（2）处理特殊种类的个人信息是数据控制者为了履行权利义务所必须；（3）处理行为是为了保障个人信息主体或其他自然人的重要利益；（4）处理行为在非营利组织保护下，为从事合法活动所执行的；（5）为了实质公共利益所必须；（6）为了预防或职业医学所必须；（7）为公共健康领域的公共利益所必须；（8）为公共利益、科学历史研究或数据目的进行存档等。

值得注意的是，GDPR 在信息收集环节强调了个人信息主体在自由不受干扰的情况做出同意的重要性，这一问题几乎在所有法域都可能会涉及。具体而言，GDPR 第 7 条第 4 款明确规定同意应是自由做出的（freely given），实践中，GDPR 成员国的数据保护机构也已经依据该条向某些组织开出了罚单。例如，在 Anderstorp 一案中，Anderstorp 中学在教室里安装了一部人脸识别相机以提升登记学生考勤的效率。瑞典数据保护机构认为，尽管学校获得了学生及其监护人关于在教室收集学生人脸识别信息的同意，但是该同意在 GDPR 下并不合法有效。因为学生在学校接受教育，导致学校与学生及其监护人的地位不平等，并不能充分体现学生及其监护人的自由意志，因此并不满足 GDPR 对于个人信息主体自由做

[6] 澳大利亚《隐私法案》第 6C 条：organisation means: (a)an individual; or (b)a body corporate; or (c) a partnership; or (d) any other unincorporated association; or (e) a trust; that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory。

[7] 澳大利亚《隐私法案》，第 3.3 条、第 3.4 条。

出同意的要求。据此，关于个人信息主体的同意是否自由做出，需要企业在不同场景下具体分析，此点值得注意。

（三）信息存储

对于人脸信息的存储要求，美国伊利诺伊州 BIPA 以及德克萨斯州《生物标识符的获取及使用》（《商法典》第 503 章）的规定较为详细全面。尽管具体细节不同，两个法案皆从信息存储保护保护措施与保存时长、销毁要求等角度进行了规定。

BIPA 要求企业在已满足收集生物识别信息的初始目的，或与个人信息主体最后一次互动的三年内（以先发生者为准），永久销毁信息。[8]德克萨斯州的法案要求原则上不迟于收集生物标识符的目的完成后的一年内销毁生物标识符，除非其他法律有不同要求（例如雇主出于安保目的收集生物标识符，则假定收集数据的目的在雇佣关系终止时到期）。[9] 除前述角度外，BIPA 同时要求，拥有生物识别信息的企业应确立书面政策，并向公众公开明确存储的时限、销毁时间等。[10] 笔者注意到，仅在合理必要的范围内保存生物识别信息，几乎是所有法域普遍达成的共识，这也符合个人信息保护的基本原则--必要性原则的要求。

企业是否按照法定要求存储与删除个人信息，具有重要意义。实践中，也已经出现企业因不遵守相关法域的数据保护要求而遭受起诉的案例，应当引起企业充分重视。例如，2020 年 4 月 2 日，两名伊利诺伊州居民对 Google 提起诉讼，指控 Google 违反 BIPA 以及联邦《儿童在线隐私保护法》（以下简称“COPPA”）。该案件中，Google 向美国中小学捐赠配备“G 教育套件”的笔记本电脑，在学生使用时，Google 会创建、收集、存储和使用他们的面部及语音信息并访问联系人名单在内的其他个人信息。但是，Google 并未征求孩子或监护人同意，亦未公开发布信息保留时间或是互动结束后三年内永久销毁生物识别信息，此类做法不满足 BIPA 下的数据存储及销毁要求，从而引发了争讼。

[8] 伊利诺伊州《生物信息识别隐私法案》（BIPA），第十五节（a）条。

[9] 德克萨斯州《生物标识符的获取及使用》，第 503.001 节第（c）条。

[10] BIPA，第十五节。

需要特别注意的是，部分法域规定了数据存储本地化的要求。例如，根据印度《个人数据保护法（草案）》，满足特定条件的情况下，敏感个人信息可以传输至境外转移到印度以外，但该等敏感的个人资料应继续存储在印度。[11]

（四）信息使用

关于通过人脸识别技术获取的信息应当如何使用的问题，各法域规定之间具有共性，但也存在结合各法域实际情况而制定的独立规定。在共性层面上，主要体现为，要求数据控制者采取合理有效的措施，保障生物识别信息的安全性，同时需要将生物识别信息的使用范围限制在合理必要的范围内等。例如，美国华盛顿州要求，获取生物标识符的个人或实体应采取“合理措施”防止针对标识符未经授权的访问、使用生物识别信息的方式应与征得信息主体同意时所告知的目的一致等[12]。 又如，美国德克萨斯州要求，信息获取主体应采取合理的与存储、传输保密信息同等或更安全的措施保护生物识别符等。[13]

在个性层面上，各法域不同的社会背景决定了其特殊的考量。例如，美国《加州人脸识别技术法案》鼓励人脸识别技术的发展，针对实践中的难题，法案进行了相关回应：首先，针对人脸识别技术的准确性以及可能产生的不准确性，法案要求数据处理者提供独立测试所需的应用程序，以确保人脸识别服务不出现种族上的差异；若存在差异且已披露给数据处理者，处理者应采取措施减少差异带来的影响；[14]其次，数据控制者在依据数据做出重大决定时，应确保该数据得到了实质性的人工审查；[15]最后，数据控制者应定期对于处理及使用人脸识别技术信息的个人进行培训等。[16] 以上诸多创新之举，意在推动人脸识别技术的运用，符合加州人脸识别等信息技术产业发达的社会环境，相关落地措施值得其他法域借鉴。

（五）信息的委托处理、共享、转让与公开披露

[11] 印度《个人数据保护法草案》（2019），第 33 条。

[12] 美国《华盛顿州修订法典》，RCW 19.375.020，第（4）、（5）条。

[13] 德克萨斯州《生物标识符的获取及使用》，第 503.001 节第（c）条。

[14] 加利福尼亚州《加州人脸识别技术法案》（Assembly Bill No.2261），1798.310(a)。

[15] 加利福尼亚州《加州人脸识别技术法案》（Assembly Bill No.2261），1798.310(f)。

[16] 加利福尼亚州《加州人脸识别技术法案》（Assembly Bill No.2261），1798.310(h)。

各法域对于人脸信息的委托处理、共享、转让与披露都有十分严格的限制。以美国为例，各州的相关法案原则上禁止数据控制者出售、出租或披露通过人脸识别技术获得的信息，除非具有例外情况。各法域对于例外情形的规定存在共性，但也存在差异。

例如，伊利诺伊州 BIPA 要求符合以下三类情况之一：（1）获得了个人信息主体的同意；（2）为了完成个人信息主体所要求的金融交易；（3）根据法律要求、法院传票要求的披露等。[17]

德克萨斯州则要求符合以下情形之一：（1）信息主体同意在其失踪或死亡的情况下进行披露；（2）该披露完成了信息主体所要求或授权的金融交易；（3）该披露是联邦法规或《政府法规》第 552 章以外的州法规所要求或允许的；或者（4）出于执法目的，由执法机构或有授权的执法行动进行披露。[18]

华盛顿州要求符合以下情形之一：（1）是信息主体订阅产品或服务所必要、信息主体要求或明确授权；（2）是实现、管理、执行或完成信息主体所请求、发起或授权的金融交易所必要的，并且披露对象的第三方对该生物标识符进行了保密，并且不再进一步披露；（3）由联邦法律、州法律或法院命令要求或明确授权；（4）披露对象的第三方通过合同保证不会将本生物标识符进一步披露，也不会出于与通知和同意不符的商业目的而将其加入到数据库中；或（5）旨在准备诉讼、响应或参与司法程序等。[19]

二、我国大陆境内对人脸识别信息的监管态度

我国大陆地区对于人脸识别技术的规制，目前并没有专门统一的法律或指引，因此人脸识别信息通常受到个人信息保护的一般法律规制，这些规范中可能会就生物识别信息进行特殊的规定。其中既包括《网络安全法》、《数据安全管理办法（征求意见稿）》等法律法规，也包括《国标》等重要的个人信息保护国家及行业标准等。笔者理解，整体上，我国目前对于人脸识别信息的一般及特殊监管规则涉及数据的生命周期，整体较为严格，但是效力层级可能不高。

[17] BIPA，第十五节（d）条。

[18] 德克萨斯州《生物标识符的获取及使用》，第 503.001 节第（c）条。

[19] 美国《华盛顿州修订法典》，RCW 19.375.020，第（3）节。

根据《国标》，面部识别特征属于个人生物识别信息，归属敏感个人信息，因此对其的保护水平相较一般的个人信息也会更高。[20] 例如，在信息收集环节，《国标》要求单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意。[21]《数据安全管理办法（征求意见稿）》第十五条要求网络运营者以经营为目的收集重要数据或敏感个人信息的，应向所在地网信部门备案。备案内容包括收集使用规则，收集使用的目的、规模、方式、范围、类型、期限等，不包括数据内容本身。

近期发布的《个保法草案》则在体例上区分了个人信息处理的一般规则和针对敏感个人信息的特殊处理规则。《个保法草案》第二章第二节用四条规定了针对敏感个人信息的处理，但没有使用生物识别信息的措词。其中，第二十九条规定了敏感个人信息的定义和处理敏感个人信息的原则要求。根据该条，个人生物特征属于敏感个人信息，同时敏感个人信息还包括了个人行踪信息。处理敏感个人信息必须具有特定、充分必要的目的。另根据第三十一条，处理敏感个人信息时，应当向个人信息主体告知《个保法草案》第十八条规定的事项（即处理一般个人信息时应当向个人信息主体告知的事宜）以外，还应当告知处理敏感个人信息的必要性以及对个人的影响。

根据《个保法草案》第三十条，“基于个人同意处理敏感个人信息的”，应当取得个人的“单独同意”。合理推断，处理敏感个人信息的合法性事由不仅仅包括同意，可能还包括《个保法草案》第十三条规定的其他合法性事由，例如订立或履行合同所必需等。由此，处理敏感个人信息的企业可能在适用合法依据这一层面具有一定的自主权，在无法获取用户同意的情况下，只要其能够合理论证证明满足其他合法事由，并且严格履行了其他合规措施，如进行个人信息安全影响评估等，则可以满足处理敏感个人信息的正当性要求。针对同意的形式以及 “单独同意”和“书面同意”具体构成要件，可参见本报告第一部分，此处不再多余赘述。

此外，需要注意的是，《个保法草案》还对公共场所安装图像采集设备的场景进行了特殊规定。根据第二十七条，公共场所安装图像采集设备，需要设置显著标识，并且仅可用于维护公共目的，一般情况下不得公开或向他人提供。此条

[20] 《信息安全技术 个人信息安全规范》，第 3.2 条和附录 B。

[21] 《信息安全技术 个人信息安全规范》，第 5.4 条第（c）款。

针对在小区、商场等公共场所安装摄像头设备的企业或其他组织需要尤其关注。但从体例上来说，该条属于第二章第一节的一般规定，同时还需要结合第二章第二节规定的“敏感个人信息”进行综合理解。

在信息存储方面，《国标》指出，个人生物识别信息应与个人身份信息分开存储，且原则上不应存储原始个人生物识别信息。[22]

在信息使用方面，《国标》对于个人敏感信息的访问与修改做出了明确规定，建议数据控制者按照业务流程的需求出发操作权。[23]且在注销账户的过程中需要收集个人敏感信息核验身份时，应明确对收集个人敏感信息后的处理措施，如删除或匿名化等。[24]

在信息的共享、转让与公开披露方面，《国标》原则上禁止个人生物识别信息的共享、转让。如确需共享、转让的，应单独向个人信息主体告知目的、涉及的个人生物识别信息类型、数据接收方的具体身份等信息，并征得明示同意。[25]当然，在特定具有正当事由的情况下，共享、转让和公开披露无需征得个人信息主体授权同意。除了在不同阶段的数据生命周期进行监管，《国标》同时对于个人信息安全事件处置以及组织的个人信息安全管理要求做出了规定等。

目前，我国已经出现企业使用人脸识别技术的案例。在郭兵诉杭州野生动物世界案中，消费者郭兵认为，杭州野生动物世界强制消费者注册账号，提供人脸识别信息核验身份，违反了收集个人信息的必要性原则，动物世界可以找到其他替代性的核验消费者身份的方式。目前该案已经被杭州市富阳区人民法院受理。[26]未来我国对于人脸识别技术的监管和司法态度如何，还有待进一步的执法和司法案例来判断。

三、境内外监管经验带来的启示

正如开篇所说，人脸识别技术的发展带来了效率与商业价值的红利，然而这把双刃剑同时也给公众个人隐私及个人信息安全带来了挑战，亟待立法与技术的

[22] 《信息安全技术 个人信息安全规范》，第 6.3 条。

[23] 《信息安全技术 个人信息安全规范》，第 7.1 条第（e）款。

[24] 《信息安全技术 个人信息安全规范》，第 8.5 条第（e）款。

[25] 《信息安全技术 个人信息安全规范》，第 9.2 条第（i）款。

[26] https://www.sohu.com/a/351559322_382470，最后访问于 2020 年 11 月 6 日。

发展进行解决。尤其是，考虑到我国政府目前大力推行人脸识别技术发展的宏观背景，这些问题未来需要解决的紧迫程度将会更加突出。这需要我们考虑技术本身的特点与实际商业应用，结合境内外的监管经验，在规避技术缺陷、防范技术滥用方面作出更多探索。

基于上文的分析，我国目前存在对使用人脸识别技术在整个生命周期的规定相对较为粗略，整体上偏于宏观，缺少细节性的指导意见，在某些环节（例如共享、存储与销毁等）还缺乏关于生物识别信息的特殊规定。例如，在不同应用场景下企业如何把握收集敏感个人信息的必要性、如何判断用户被给予了充分的选择权和拒绝权、如何构成有效的“同意”以及存储时间是否可以更加细化。这些都将有赖于未来的法规细则和标准进行进一步说明。

笔者推测，未来我国政府对企业人脸识别技术的发展持积极态度，但是该积极的程度可能需要根据国情来把握，会像美国加州、伊利诺伊州一样采取相对宽松的态度，还是会像华盛顿州等保守中立，需要结合我国国情进行进一步判断。但是，这不妨碍我们参考美国《加州人脸识别技术法案》、BIPA 等法案中的亮点，来细化我国的相关规定。例如，考虑到环境、种族、光线等因素会影响到人脸识别的准确性，对于人脸识别技术可能产生的偏差以及由此带来的不公平待遇，是否可以考虑提出相关要求，例如进行人工审查以防止自动化决策给个人信息主体带来的影响等。

又如，对于数据的存储与销毁环节，除了目前“实现目的所必需的最短时间”的一般性规定以外，我国是否需要借鉴伊利诺伊州及德克萨斯州的法案都对于生物识别数据具体存储时间与销毁要求（最长存储时间的如一年、三年等）也值得考量。我国目前在其他敏感个人信息的监管规则中其实具有类似的规定，如在个人金融信息保护领域，可能出于反洗钱的目的，要求金融机构在交易结束后 5 年内保存相关个人金融信息等。这一方式是否需要、以及如何运营到生物识别信息或者人脸识别信息的监管规则上，有待立法者的思考和进一步的观察。

除此之外，人脸识别技术获取的面部识别信息与其他生物数据最大的不同在于其非接触型的信息获方式。虹膜、指纹、掌纹等的获取或多或少需要数据采集者与个人信息主体有实质接触，然而面部识别信息则可轻易通过设备获得，无需接触。尽管各法域的监管可能都将获取个人信息主体的同意作为收集处理个人信

息的正当性事由，但在人脸信息的场景下，企业如何履行该义务、如何构成有效同意，可能有赖于未来立法和执法中的进一步解答。

除了以上在法律法规细化层面的讨论外，从长远看，我国人脸识别技术的技术标准正在制定中，这将会给人脸识别技术的运用与处理人脸识别信息的行为带来更具有实践意义的参考。如何把握企业经济运行的客观需求和人脸信息保护的平衡点，我们需要实践中不断探讨。

四、结 语

法国哲学家福柯在其著作《规则与惩罚》中，用圆形监狱（Panopticon）作为隐喻，认为我们活在无处不在的监视中，从而潜移默化被改造着，这是对人自由意志的巨大摧残。福柯可能未曾预见人脸识别技术的发展与应用，四十年后的今天当我们重新审视科技带来的挑战时，或许这样的担忧更为迫切。如果人脸识别科技不能向善，带来的伦理与人权的损害无疑将是巨大的。

本文对目前代表性法域的人脸识别技术的监管规则做了简要的梳理与概括，并就域外法中可借鉴的经验进行了初步理解。值得注意的是，随着科技的不断进步，人脸信息仅属于敏感个人信息/生物识别信息的一种，未来我国会逐步重视对其他敏感个人信息/生物识别信息的监管，届时笔者会进一步分析，与大家一同分享。

第二篇：关于告知与同意的合规要求

告知同意原则是《个保法草案》中数据主体处理个人信息的一项重要合法性依据，贯穿于数据生命周期的各个阶段。纵观全球各国个人信息保护立法，也普遍采用了该原则作为处理个人信息的合法事由（或之一）。尽管不同法域的法律法规对于“同意”的具体履行方式、需履行告知义务的主体等方面的规定存在差异，但基本对于将其作为收集处理个人信息的重要前提达成共识。欧盟在 1995 年公布的《个人数据保护指令》中就已规定采集个人信息应告知个人信息主体，并在 2016 年发布的 GDPR 第 4 .11 条中进一步明确了构成有效“同意”的要求，包括明确向个人信息主体进行告知的意愿表达应是自由给出的、特定的等。WP29 则出台《GDPR 同意指南》（*Guidelines 05/2020 on consent under Regulation 2016/679*）, 对 GDPR 的告知同意原则作出深入解读。《日本个人信息保护法案》（“APPI”）要求提前披露收集个人信息的目的并获取个人信息主体同意，超出事先同意的范围处理使用个人信息的，应获得再次同意，并且在收集敏感个人信息前应获得个人信息主体明示同意。《美国加州消费者隐私保护法案》（“CCPA”）则要求在收集消费者个人信息前告知消费者收集的个人信息类型及目的。

《网络安全法》第四十一条和《民法典》第一千零三十五条对于收集处理个人信息前获得明示同意这一原则做出了纲领性的规定，《个保法草案》第十四条至十八条对于获得个人信息主体同意的构成要件、告知的具体内容、个人信息主体撤回同意的权利和无需告知或应当保密情形下的例外作出了规定。除上述法律外，《国标》针对基本业务功能及附加业务功能进行了告知同意方式的细分。2020 年 1 月，全国信息安全标准化技术委员会发布了国家标准《信息安全技术 个人信息告知同意指南（征求意见稿）》（以下简称“《指南（征求意见稿）》”）。该推荐性国家标准虽仍在征求意见中，但其不仅对于告知同意原则作出了阐述，并对不同场景下告知同意的可实现性做出了详细解释，是企业与平台开展告知同意合规工作的重要且有益的参考。

该原则的含义并不难理解，但实践中的个人信息收集与使用的场景千变万化，如何有效得履行告知义务并获取有效同意实为一个较棘手的问题。本文将结合上述法律法规及国家标准中对于告知同意原则的要求，实践中告知同意机制的设计，

特殊场景中的同意告知实现及欧盟 GDPR 下告知同意的规定，对于告知与同意的合规要求作出更为细化的解读。

一、需要告知同意的场景及告知的具体内容

正如上文所说，告知同意原则贯穿于数据生命周期的各个环节，在个人信息的收集、委托处理、共享、跨境传输等环节都有需告知用户并获取同意的场景。法律法规对于不同场景下告知同意的例外作出了规定，给予个人信息控制者一定的自主控制空间。清晰地了解需告知用户并获取同意的触发场景对于企业与平台履行告知同意合规要求十分重要，笔者主要将需要告知同意的场景及其例外总结为以下四大类：

需要告知同意的场景	具体案例	该场景下免于告知的情形（例外）[27]
1. 收集使用个人信息	• 个人信息主体**主动提供**（填写、上传等）个人信息； • 通过 SDK、API、传感器等采集个人信息； • 通过与**用户交互**记录个人信息主体行为的； ……	• 与个人信息控制者**履行法律法规规定的强制性义务**相关的； • 与国家安全、国防安全直接相关的； • 与公共安全、公共卫生、公共网络安全、网络环境治理、重大公共利益直接相关的 ……
2. 使用目的变更时	• 超出原有授权范围应用于**新的业务场景**的； • 间接获取个人信息后，进行**加工处理形成新的个人信息**并用于其他目的； • 所提供的产品或服务基于业务扩展而增加的**新的功能**，该新增功能收集使用个人信息都超出原授权范围的； ……	• 新设目的与原先授权目的**有直接或合理的关联**，个人信息控制者采取类似的处理规则和安全保护措施； • 服务升级、改造后**使用个人信息的频率、用户画像计算和展现方式、与个人信息主体的互动方式发生调整**的； • 将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，且使用对外提供学术研究或描述的结果时，对个人信息进行**去标识化处理**的； ……

[27] 此处为代表性列举，完善的列举请参考《指南（征求意见稿）》第 6 章。

3. 对外提供个人信息时	• 应业务所需**向第三方共享**个人信息； • 应业务变更等原因，**向第三方转让**个人信息，且不再保留个人信息； • 以不定向方式向**公众公开披露**个人信息； ……	• 与**国家安全、国防安全**直接相关的； • 与**公共安全、公共卫生、重大公共利益**直接相关的，例如在发生大规模地质灾害的紧急情况下，向有关人员的亲属、行政机关和救援部队提供受灾人群、伤亡人员的个人信息； • 与**犯罪侦查**直接相关的，例如金融机构为配合公安机关调查某金融犯罪，依据有效法律文书向公安机关提供嫌疑人交易流水信息； ……
4. 其他情形	• 涉及**个人信息出境**的情形； • 个人信息处理规则，如隐私政策，内容发生对个人信息主体权益产生影响的**实质性变化**时； • 个人信息主体**撤回授权**同意时； ……	

《个保法草案》第十八条列出了个人信息处理者应向个人告知的事项：（1）个人信息处理者的身份和联系方式；（2）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；（3）个人形式本法规规定权利的方式和程序；（4）法律法规规定应当告知的其他事项。在具体实践中值得注意的是，不同的数据生命周期需告知个人信息主体的内容也不相同，需根据不同场景额外披露可能对于个人信息主体权利造成影响的信息，这也与《个保法草案》中的第十八条第四项相呼应。以对外共享为例，个人信息控制者还应告知第三方企业收集实施者、收集内容、使用目的、收集时间、保护措施等相关的信息。

二、有效告知同意：合规要求与措施

（一）通过用户设计实现充分的告知

1. 清晰、易懂的语言

《个保法草案》第十四条中明确指出个人的同意应在“**充分知情**”的情况下作出，并在第十八条中指出了应以“**显著方式、清晰易懂的语言**”向个人信息主

体告知。因此告知同意合规性的重要措施之一则应做到充分告知个人信息主体。由于个人信息控制者自身产品和/或服务各式各样，因此在履行充分告知义务时，应考虑产品 UI 交互时的具体情况，并采用用户易于理解的语言表达进行信息披露，这一要求需要企业及平台重点关注用户交互授权界面的设计。除此之外，（1）敏感个人信息和/或（2）个人信息处理规则等告知内容发生重大变化的，应该做到**明确表示或突出显示**。实践中通常采取的做法包括在隐私政策及用户服务协议中对于重点提示的内容进行加粗、斜体以做加强性告知。针对特殊群体，除文本外，应提供图片、语音或视频等内容对告知内容进行阐述。这一要求同时也在司法实践中得到印证。如在上海某信息技术有限公司、邢某网络购物合同纠纷案中，法院认为该公司虽然在 App 中设置了“已阅读并同意服务协议与隐私政策”模块，但该模块为浅灰色字体并标注于页面底端，未以明显的方式提示消费者，因此对于邢某主张协议无效予以支持。

这一要求与 GDPR 第 12.1 条中的规定基本一致，GDPR 要求数据控制者应以“简洁、透明、易懂且容易获取的形式，使用清楚且直白的语言”提供有关数据处理的信息。WP29 在《关于 2016/679 号条例下“透明”的指导方针》（*Guidelines on Transparency under* Regulation *2016/679*）中对于“简洁、透明、易懂”作出深入解读，将其核心含义阐释为“数据主体应当能够（通过控制者披露的信息）事先确认对其个人数据的处理的范围和后果，且不应在此后对其个人数据的使用方式感到意外”。法国国家信息与自由委员会（“CNIL”）在 2019 年发布公告，对谷歌未尽控制者披露义务处以 5000 万欧元的罚款。CNIL 指出，谷歌在其隐私政策中采用了过于笼统且模糊的说法，如“为了在内容上提供个性化服务”、“收集信息用于改善向所有用户提供的服务”等，用户无法根据上述信息充分理解其所执行的处理操作，违反了 GDPR 第 12.1 条的要求。

2. 用户友好的展示方式、告知频率与时机

在设计充分告知机制时，需要注意的另一项要求，则是信息披露的**展示方式**。在数字经济时代，各类移动终端设备都会涉及个人信息的收集使用，除了常见的 App（软件）收集个人信息之外，常见的还包括 PC、智能穿戴设备和智能家居设备等硬件设备、操作系统对个人信息的收集。EDPB 于 2020 年 1 月发布《在车联网和交通相关应用程序场景中处理个人信息的指南》（*Guidelines 1/2020 on*

processing personal data in the context of connected vehicles and mobility related applications Version 1.0）指出，在车联网场景相关的数据处理活动中，取得用户同意应当是核心。因此，企业与平台都应根据自身产品和/或服务的不同对信息披露的可读性和有效性通过展示方式作出相应调整：

设备终端	展示方式
PC 端	• 弹窗窗口和下拉列表
移动端	• 由于设备屏幕较小，应采取多层次的告知同意模式，通过以简短内容（包含图示和文字）告知关键内容，并提供完整版链接
IoT 设备端	• 在链接互联网时通过绑定该设备的移动端程序展示告知内容 • 如设备显示屏足以展示告知内容，可在自带的显示屏上进行展示
书面	• 将核心告知内容布置于签字确认区域附近

除了清晰易懂的语言表述与便于阅读的展示方式外，另一需要注意的合规要点为：**告知的时机、**频率**与方式**。《指南（征求意见稿）》提出“应用软件的告知时机与频率应与用户体验感及舒适度相平衡”，《国标》更是明确指出“除非个人信息主体主动选择开启扩展功能，在 48h 内向个人信息主体征求同意的次数不应超过一次”。告知的方式也应根据告知的场景不同而采取不同措施，如当告知的场景为使用目的变更、对外提供个人信息或个人信息处理规则发生变化时，宜用弹窗、浮窗、短信、邮件、消息推送等显著方式进行告知；当告知的场景为临时性的个人信息处理行为（如发生个人信息安全事件、产品或服务停运等），可以采取邮件、短信的方式告知。

（二）如何获得有效同意

告知同意合规的另一重要方面为获得用户的有效同意。《个保法草案》提出“单独同意”与“书面同意”的概念，并明确了需要单独同意的场景（具体可参考本报告第一部分第 7 章）。在《国标》及《指南（参考意见）》中，需要特别注意的是“授权同意”与“明示同意”的区分。**授权同意**，指的是“个人信息主体对其个人信息进行特定处理作出明确授权的行为，包括通过积极的行为作出授权（明示同意），或通过消极的不作为而作出授权”；**明示同意**，指的是“个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或自主作出肯定性动作（如主动勾选、主动填写等）对其个人信息进行特定处理作出明确授权

的行为”。需要用户明示同意的场景包括涉及敏感个人信息、个人信息控制者因业务需要使用目的变更、个人信息控制者向第三方共享、转让个人信息等。

GDPR 第 4.11 条中将“同意”定义为“数据主体通过声明或明确的肯定性行为作出的自愿、具体、知情且明确的指示。通过声明或明确肯定的行为作出的这种指示，意味着其同意与他或她有关的个人数据被处理。”当某项处理活动存在严重的数据安全风险时，数据控制者需要获得数据主体的明示同意（explicit consent），适用的场景主要包括自动化决策、用户画像等。WP29 在《GDPR 同意指南》中将“具体”这一要求进一步解读为，数据控制者应针对每项处理目的提供单独“选择加入”选项，以确保用户能够就特定的目的给出具体的同意。上述 CNIL 处罚谷歌的案例中，CNIL 指出用户给出的同意并不是具体的，因为用户被要求同时勾选“我同意谷歌的服务条款”和“我同意按照上述方式和隐私政策中进一步解释的方式处理我的信息”，对于谷歌数据收集处理的所有目的（包括个性化广告、语音识别等）作出了一揽子的授权。由此可见，GDPR 下的有效同意相较中国目前的规定而言更为严格，且在隐私政策的勾选方式上也是采取了更加具体的思路。

（三）告知同意的保存及改变同意的范围、撤回同意

获得用户的有效同意不能免除企业的其他合规义务，个人信息控制者（即《个保法草案》中所称的个人信息处理者）还需保障用户改变其同意范围和撤回同意的权利。《个保法草案》第十七条提出“个人信息处理者不得以个人不同意处理其个人信息或者撤回对其个人信息处理的同意为由，拒绝提供产品或服务；处理个人信息属于提供产品或服务所必需的除外。”因此，企业与平台在其开发的产品和/或服务中应注意设计明显的权利实现途径并在隐私政策中作出相应的披露。《GDPR 同意指南》将保障改变同意范围、撤回同意的权利与获得有效同意的要求相结合，指出数据控制者应当充分保证数据主体可以在不受损害的情况下拒绝或撤回同意。如果数据控制者能够证明可以允许数据主体撤回同意，且撤回同意后不会产生任何不利后果（例如不会降低服务质量而损害数据主体权益），才足以证明数据主体的同意是自由做出的。

《指南（征求意见稿）》同时指出只要处理个人信息的活动持续存在，个人信息控制者证明告知同意的义务就持续存在。因此，个人信息控制者应按照要求

留存告知同意的证据，包括时间、事项、目的等，针对可能产生高风险的个人信息收集行为，还应留存具体的告知同意。在个人信息处理活动结束后，证据的留存不应超过履行法律义务、提起或应对诉讼、纠纷的必要限度（如以诉讼时效为限）。GDPR 第 7.1 条也作出了同样要求，即“控制者需要能证明，数据主体已经同意对其个人数据进行处理”，但 GDPR 并未对于证明的方式及同意的持续期限进行规定。

三、未成年人个人信息的告知同意

目前，线上教育平台、网络游戏等主要面向未成年人用户的产品和/或服务发展蓬勃，因此如何满足处理未成年人个人信息的告知同意要求，为实务中常遇到且需重视的问题。《个保法草案》第十五条做出了处理未成年人个人信息的特殊同意要求，这与《儿童个人信息网络保护规定》第九条中的规定相呼应，即“网络运营者收集、使用、转移、披露儿童个人信息的，应当以显著、清晰的方式告知儿童监护人，并应当征得儿童监护人的同意。”虽然《个保法草案》第十五条中增加了“个人信息处理者知道或应当知道”的前置情形，一定程度上减轻了个人信息控制者的责任，但企业需论证确实不知悉个人信息主体为未成年的情况。特别是根据法律法规，某些企业与平台必须采取实名制认证机制的，要证明其并不知悉是儿童用户，可能较为困难。

《指南（征求意见稿）》附录 A 具体阐述了未成年人及其监护人身份验证的方式，同时指出在核验时应充分考虑不同产品和/或服务在受众群体上的本质差异，以减少对用户不必要的打扰。如手机银行等未成年人为非主要受众的产品，可通过弹窗问询是否已满 14 岁，而游戏、社交等产品则宜采取验证强度较高的方式，如输入生日、身份证号等，但不宜超过必要限度。然而值得注意的是，在《个保法草案》增加“推定知情”前置的情况下，企业自证的义务与（指南（征求意见稿））中提出的验证方式如何配适，还有待进一步的观察。

四、总结

“告知同意”要求需要企业与平台从用户自主自决权出发，充分考量产品的用户设计与交互页面，以确保告知的充分性与同意（包括撤回同意）的有效性。上文通过解读告知的方式、触发时机、告知内容、有效同意构成要件等各个方面，

对告知同意的合规要点进行剖析，希望能作为企业与平台在设计告知同意机制时的有效参考。同时，笔者也将紧密关注《指南（征求意见稿）》的最终出台及《个保法草案》的后续发展，将在后续向大家提供更为完善的告知同意合规要求解读，以供交流与探讨。

第三篇：关于个人信息控制者和处理者合规要求

一、本文术语采用

如本报告第一部分所述，《个保法草案》并未采取《国标》中对“控制者”的定义，而是采取了和《民法典》“个人信息处理者”相同的术语表述。考虑到《个保法草案》本身没有对受委托的“处理者”这一数据采用替代的词语，因此为了避免混淆，本篇文章所指的“数据控制者”、“数据处理者”的概念将先与 GDPR 中的术语保持一致，以便理解。

《国标》	《个保法草案》	GDPR	本文采用术语
个人信息控制者	个人信息处理者	数据控制者	个人信息控制者
共同个人信息控制者	共同决定的个人信息处理者	共同控制者	个人信息共同控制者
受委托处理数据者	受委托处理数据者	数据处理者	个人信息处理者

二、个人信息控制者、共同控制者与处理者的身份界定

（一）个人信息控制者

《个保法草案》第六十九条的规定，“个人信息处理者”是指“自主决定处理目的、处理方式等个人信息处理事项的组织、个人”。根据《国标》第 3.4 条的规定，“个人信息控制者”是指“有能力将决定个人信息处理目的、方式等的组织或个人”。综合前述两种定义可知，判断组织或者个人是否为控制者的核心要点为（1）“自主”（2）“决定”（3）“目的、处理方式”（4）“个人信息处理事项”以及（5）“组织、个人”。本节将针对这五个要件进行讨论。

1. 自主

《个保法草案》或者其他已公布的法律法规、国家标准并没有明确这里的“自主”指的是实体完全根据自己的意思自治决定个人信息的处理，还是同样包括根据法律要求处理个人信息的情况，例如当法律直接赋予某组织收集和处理个人信息的职责时，该组织是否构成个人信息控制者，如通过行政授权某一非国家机关

执行公共任务，这一点可能要留待以后针对《个人信息保护法》的司法解释或者配套的法律文件进行明确。参考 EDPB 于 2020 年 9 月 2 日发布的《GDPR 项下数据控制者与数据处理者概念的指南》（Guidelines 07/2020 on the concepts of controller and processor in the GDPR，以下简称“《EDPB 指南》”）的说明，法律直接制定任务或者赋予收集和处理某些数据的职责时，即间接地规定了谁是控制者。例如，法律规定某公共机构有义务提供社会福利，如根据公民的财务状况向其支付款项。为了执行这些付款，公共机构必须收集和处理有关申请人财务状况的数据。即使法律没有明确规定市政当局是该处理程序的控制者，但属于根据法律规定而进行的推定。在这种情况下，即便个人信息处理的目的由法律决定，而非组织或者个人自主决定，该公共机构仍然构成个人信息控制者[28]。

2. 决定

这里的“决定”应当理解为不仅包括实际选择或者决定了个人信息处理事项的主体，还包括客观有能力控制或者调整个人信息处理事项的主体。例如，当 App 中嵌入自主收集个人信息的 SDK 时，由于个人信息收集和处理的范围由 SDK 自主决定，同时 SDK 又通过外露自身品牌对外宣示自己有自主决定权，自然构成个人信息控制者，但由于 App 从客观上有能力在后台开启或者关闭 SDK 收集个人信息的通道或者接口，因此即便 App 没有实际参与到 SDK 收集个人信息的过程（甚至不能看到 SDK 收集了哪些个人信息），App 也仍然构成个人信息控制者。

3. 目的、处理方式等

这里的“目的”、“处理方式”之间的应当采“或者”之意。只要组织或者个人决定了个人信息处理事项其中任何关键事项，则构成个人信息控制者。如果是两个以上的实体一同决定某一个人信息处理的事项时，则各主体间构成“个人信息共同控制者”。关于“个人信息共同控制者”的说明参见本文第二部分第（二）节。

4. 个人信息处理事项

前述的“目的、处理方式”需要与个人信息的处理相关。根据《个保法草案》第四条第二款的规定，“个人信息的处理包括个人信息的收集、存储、使用、加

[28] 《EDPB 指南》第 22 段。

工、传输、提供、公开等活动”。那么只要组织或者个人的处理活动符合前述的行为之一，则满足此要件。

5. 组织、个人

该构成要件涉及可以成为控制者的实体类型。根据《个保法草案》的规定，个人信息控制者可以是“组织、个人”，没有局限于组织，此处与《国标》的规定相似。但对于个人担任控制者的情形，则需要与组织中的主要负责人相区分开。换句话说，处理个人信息活动时的控制者并不是组织的负责人个人（如 CEO），而是组织本身需要对外承担相关责任。如果主要负责人故意或者过失没有尽到职责范围内的义务，则应根据相关条款追究主要负责人或者直接责任人的责任。《个保法草案》第六十八条同样特别提示自然人因个人或者家庭事务而处理个人信息的不适用本法，限缩了自然人受制于《个保法草案》的范围。

此外，这里的“组织”并没有明确是否仅局限于一般性的私营主体。但根据《个保法草案》第三节“国家机关处理个人信息的特别规定”，国家机关的个人信息处理行为也适用《个保法草案》，履行相关的合规义务。

（二）个人信息共同控制者

《个保法草案》并没有明确采用“共同控制者”或者类似的术语。但根据《个保法草案》第二十一条的描述，即为“两个或者两个以上的个人信息处理者共同决定个人信息处理的目的和处理方式”，实际涉及了此类情况。根据该项描述，当两个或者两个以上的实体共同决定个人信息处理的目的和方式时，则该等实体构成个人信息共同控制者，判断的核心要点在于“共同控制”这一要素。《个保法草案》没有对何种方式构成“共同”进行说明。实践中可能存在两种情况：一种为个人信息处理的每一个环节均由各方共同决定。例如，某项个人信息处理行为包含 A、B、C、D 四个要点，甲乙实体共同决定采取 A1 而非 A2、共同决定采取 B1 而非 B2，以此类推。另一种方式为各实体分别决定某一因素，合并所有因素后完整的决定了个人信息的处理。例如，甲实体决定了 A、B 两个要素采取 A1 和 B1，乙实体决定了 C、D 两个要素采取 C1 和 D1。甲乙实体合并起来为 A、B、C、D 确定了各自的内容。第一种构成共同控制者的情况较好理解，但对于第二种情况是否构成共同控制者尚不明确。比如在极端的情况下，甲实体根本无权过问乙实体的决定和处理情况，是否仍然属于“共同”值得探讨。参考《EDPB 指南》中的

观点，是否构成共同控制者需要在个案中认定，且不能单纯地以使用了共同的数据处理系统或者基础设施、存在商业互利就即认定构成共同控制者。例如，当各方进行的处理可分割，且可在不被另一方干涉的背景下进行，则不构成共同控制者[29]。

（三）个人信息处理者

包括《个保法草案》在内，中国目前已经公布的法律法规、标准尚未对“处理者”这一术语进行定义，对于该术语的理解更多地是援引 GDPR 以及学界中对于处理者的定义，适用我国法律法规、国家标准中“委托处理”的相关章节中所规定的合规义务。但结合学界以及 GDPR 实践中的相关经验，处理者应当是与控制者不同的、受控制者之委托处理个人信息的实体，应当与控制者直接授权相区分[30]。当处理者的处理行为超出了控制者的指示范围，自己有权决定自己的处理目的或者处理方式时，处理者将成为控制者。

（四）合规提示

1. 个人信息控制者与处理者之间的关系

根据《个保法草案》第九条的规定，个人信息控制者对个人信息处理活动负责。从“委托行为”角度出发，也可以判断出个人信息控制者是对外承担责任的主体，如果处理者的处理违反了双方的约定或者控制者的指示，控制者承担责任后可向处理者追偿。

2. 个人信息共同控制者之间的关系

根据《个保法草案》第二十一条第二款的规定，对于共同处理个人信息的控制者需要依法对外承担连带责任。对内，共同控制者之间可以根据彼此之间的协议对于责任的约定（如有）进行内部分配。

3. 身份认定与合同签署之间的关系

虽然在实践中担任数据控制者或者处理者的多方实体间可能会签署合作协议、数据处理协议等明确各方身份，但从法律层面对于身份的认定仍需聚焦于实际的

[29] 《EDPB 指南》第 60、66 段。

[30] 《EDPB 指南》第 78 段。

处理行为中各方承担的角色，单纯的合同并不能起到决定性作用，也不能以此来规避自身的义务。

三、个人信息控制者、共同控制者与处理者的合规义务

（一）个人信息控制者的合规义务

根据《个保法草案》的规定，个人信息控制者需要履行至少以下合规义务：

1. 处理个人信息符合合法、正当、必要、公开透明、准确的原则

根据《个保法草案》第五条、第六条的规定，处理个人信息应当采用合法、正当的方式，遵循诚信原则，不得通过欺诈、误导等方式处理个人信息；应当具有明确、合理的目的，并应当限于实现处理目的的最小范围，不得进行与处理目的无关的个人信息处理。根据《个保法草案》第七条的规定，处理个人信息应当遵循公开、透明的原则，明示个人信息处理规则。

此要点为原则性要求，一方面企业要保障自身的个人信息处理的方式正当且合法，不采用误导或者欺诈的方式处理个人信息。此外，在收集个人信息之前应当具有明确的目的，并仅在最小范围内收集个人信息。为实现处理目的，保障所处理的个人信息准确，并及时更新。

2. 通过《隐私政策》或其他文件告知个人信息主体

根据《个保法草案》第十八条、第三十一条的规定，企业应当在处理个人信息前通过公开的文件（如《隐私政策》），以清晰易懂的语言告知用户如下事项：

1）.公司的身份和联系方式；

2）.个人信息的处理目的、方式、种类、保存期限；

3）.个人行权的方式和程序；

4）.其他根据其他法律、行政法规要求需要披露的事项。

5）.如果是处理敏感个人信息的，则还应当告知处理敏感个人信息的必要性以及对个人的影响。

从形式上而言，该份文件放置在显著的位置，便于用户访问、查阅和保存。

根据《个保法草案》第十九条的规定，如果根据法律、行政法规应当保密或者不需要告知的，可以不向用户告知，此条款为告知义务的例外。如存在此种情况建议公司详细记录不告知的情况、所依据的法律，以便作为日后的证据。

3. 获得个人信息处理的法律依据，特定情况下必须征得同意

根据《个保法草案》第十三条的规定，个人信息控制者只有符合下列情形的才能处理个人信息：

1）.取得个人的同意；

2）.为订立或者履行个人作为一方当事人的合同所必需；

3）.为履行法定职责或者法定义务所必需；

4）.为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；

5）.为公共利益实施新闻报道、舆论监督等行为在合理的范围内处理个人信息；

6）.法律、行政法规规定的其他情形。

以上的法律依据为并列择其一的关系，而非有一定的适用顺序。

除了上述针对一般情况的规定外，《个保法草案》还规定了某些情况下只能征求同意作为处理的依据：

1）.个人信息处理者知道或者应当知道其处理的个人信息为**不满十四周岁未成年人个人信息**的,应当取得其监护人的同意。（《个保法草案》第十五条）

2）.个人信息处理者向**第三方提供**其处理的个人信息的，应当向个人告知第三方的身份、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。（《个保法草案》第二十四条）

3）.基于个人同意**处理敏感个人信息的**，个人信息处理者应当取得个人的单独同意。法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。（《个保法草案》第三十条）

4）.**个人**信息处理者**向中华人民共和国境外**提供个人信息的，应当向个人告知境外接收方的身份、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式等事项，并取得个人的单独同意。（《个保法草案》第三十九条）

5）.取得个人单独同意或者法律、行政法规另有规定的，个人信息处理者**方可公开其处理**的个人信息。（《个保法草案》第二十六条）

6）.取得个人单独同意或者法律、行政法规另有规定的，所收集的**个人图像、个人身份特征信息方可公开或者向他人提供**。（《个保法草案》第二十七条）

7）.处理已公开的个人信息**超出与该用途相关的合理范围**的，应当依照本法规定向个人告知并取得其同意；利用已公开的个人信息从事对个人**有重大影响的活动**，应当依照本法规定向个人告知并取得其同意。（《个保法草案》第二十八条）

当企业选择以用户的同意作为处理的法律依据时，则一方面需要保证征得的同意是有效的，是用户自愿、明确作出的；另一方面需要赋予用户撤回同意的权利，并且不能以不同意处理其个人信息或者撤回其对个人信息处理的同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外（《个保法草案》第十四条、第十六条、第十七条）。

4. 存储时间符合最小期限

根据《个保法草案》第二十条的规定，个人信息的保存期限应当为实现处理目的所必要的最短时间。法律、行政法规对个人信息的保存期限另有规定的，从其规定。《个保法草案》本身没有对最短期限应为多少进行限定，而是要求企业结合处理目的进行个案判断。

5. 采取措施保障处理者处理个人信息行为安全

根据《个保法草案》第二十二条的规定，企业委托第三方处理个人信息的，需要采取措施明确委托处理的目的、方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托方的个人信息处理活动进行监督。实践中，企业可以通过与第三方处理者签订数据处理协议，明确上述要求，并对第三方处理者进行审计、尽调或者监督。

6. 保障个人信息主体的权利

根据《个保法草案》第十六条、第四章的规定，个人对其个人信息享有如下权利：

1）.知情权；

2）.查询权；

3）.决定权；

4）.更正、补充权

5）.删除权；

6）.可携带权；

7）.撤回同意权；

8）.拒绝自动化决策处理权；

9）.限制或者拒绝他人处理权；

因此，企业需要根据《个保法草案》第四十八条、四十九条的规定，根据个人的要求进行说明，并建立机制响应个人的行权请求。当拒绝个人行使权利的请求的应当说明理由。

7. 采取措施保障数据安全能力

根据《个保法草案》第五十条的规定，企业需要根据个人信息的处理目的、处理方式、个人信息的种类以及对个人的影响、可能存在的安全风险等，采取必

要措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露或者被窃取、篡改、删除，包括但不限于：

1）.制定内部管理制度和操作规程；

2）.对个人信息实行分级分类管理

3）.采取相应的加密、去标识化等安全技术措施；

4）.合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；

5）.制定并组织实施个人信息安全事件应急预案；

6）.定期对个人信息处理活动进行审计；

7）.法律、行政法规规定的其他措施。

对于各个措施的合规分析，已在报告第一部分进行详细描述，具体参见报告第一部分。

8. 任命个人信息保护负责人

根据《个保法草案》第五十一条的规定，处理个人信息达到国家网信部门规定数量的企业应当指定个人信息保护负责人，其职责为负责对个人信息处理活动以及采取的保护措施等进行监督。企业还应当公开个人信息保护负责人的姓名、联系方式等，并报送履行个人信息保护职责的部门。

对于此部分的详细分析，请参见报告第二部分第五篇文章《关于个人信息保护工作机构及负责人》。

9. 对特定数据处理进行个人信息风险评估以及记录

根据《个保法草案》第五十四条的规定，企业应当对以下个人信息处理活动进行风险评估并对处理情况进行记录，并对评估报告和处理情况保存至少三年：

1）.处理敏感个人信息；

2）.利用个人信息进行自动化决策；

3）.委托处理个人信息、向第三方提供个人信息；

4）.向境外提供个人信息；

5）.其他对个人有重大影响的个人信息处理活动。

在进行评估时，评估的内容包括以下内容：

1）.个人信息的处理目的、方式是否合法、正当、必要；

2）.对个人的影响及风险程度；

3）.所采取的安全措施是否合法、有效并与风险程度相适应。

《个保法草案》对评估以及记录做了概括性的规定，具体可以参见目前尚在征求意见稿阶段的《个人信息安全影响评估指南》。

10. 满足条件时方可将个人信息出境

根据《个保法草案》第三章的规定，只有具备了特定条件后，企业才能向境外提供个人信息，包括：

1）.通过国家网安部门组织的评估；

2）.经过专业机构的认证；

3）.与境外接收方订立合同；

4）.法律、行政法规或者国家网信部门的其他条件。

对于此部分的详细分析，请参见报告第二部分第四篇文章《关于个人信息出境的合规治理》。

11. 发生个人信息泄露时的补救与报告

根据《个保法草案》第五十五条的规定，企业发现个人信息泄露的，应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：

1）.个人信息泄露的原因；

2）.泄露的个人信息种类和可能造成的危害；

3）.已采取的补救措施；

4）.个人可以采取的减轻危害的措施；

5）.个人信息处理者的联系方式。

值得注意的是，企业采取措施能够有效避免信息泄露造成损害的，企业可以不通知个人；但履行个人信息保护职责的部门认为个人信息泄露可能对个人造成损害的，企业需要根据前述部门的要求通知到个人。

12. 对在中国境内没有实体的经营者，任命“指定代表”或设立“专门机构”

根据《个保法草案》第五十二条的规定，对于设立在中国境外，但根据《个保法草案》第三条第二款的规定受《个保法草案》约束的实体，应当在中国境内设立专门机构或者指定代表，其职责为负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。需要提醒的是该等“指定代表”或者“专门机构”并不等同于企业履行任命个人信息保护负责人的义务。

（二）个人信息共同控制者的合规义务

在第（一）部分所述控制者本身责任的基础上，如果属于共同控制者的，则根据《个保法草案》要求各个共同控制者之间需要**约定各自的权利与义务**，并对外承担连带责任。

（三）个人信息处理者的合规义务

《个保法草案》本身没有对个人信息处理者的合规义务进行专章规定，因此从适用上可能存在一定的模糊、暧昧之处。

根据《个保法草案》第二十二条的规定，除了个人信息保护原则性规定外，个人信息处理者作为受托方需要履行以下义务：

1）.按照与控制者的约定处理个人信息；

2）.不超出与控制者约定的处理目的、方式等处理个人信息；

3）.在合同履行完毕或者委托关系解除后，将个人信息返还控制者或者予以删除；

4）.未经控制者同意，不得转委托他人处理个人信息。

如前所述，《个保法草案》没有对处理者的义务进行专章规定，留待更新的草案或者正式稿中进行说明。

四、总结

2020 年是中国个人信息保护立法的关键时期，虽然在《个保法草案》出台之前，已有如《国标》等偏实践指导的文件发布规范企业承担相应的责任和义务，但《国标》究其本质仍为推荐性国家标准，且没有惩罚机制。拟出台的《个人信息保护法（正式稿）》从法律位阶上具有强制执行的效力，且规定了高昂的罚则（最高可罚五千万人民币或者年度营业额百分之五），也更具震慑力。结合欧美有关企业因违反数据保护法而被处罚的案例来看，不乏有头部企业因为未能履行个人信息保护义务遭到处罚，因此建议无论大中小企业均能做到提前布局，梳理公司数据资产、采取相应的数据保护合规措施与方案，从而避免给企业、直接负责人和员工个人带来风险。

第四篇：关于个人信息出境的合规治理要求

一、个人信息出境的界定与规制

自从《网络安全法》于 2016 年提出对于关键信息基础设施运营者的数据本地化存储义务和跨境传输的评估义务的要求，实践中就引起了监管部门和相关企业的广泛的关注。2017 年，《个人信息和重要数据出境安全评估办法（征求意见稿）》（“《2017 年办法（征求意见稿）》”）又将“限制个人信息出境”的规制主体扩大，由《网络安全法》要求的“关键信息基础设施的运营者”（“CIIO”）这一主体扩展到所有的“网络运营者”。随后于 2019 年 6 月 13 日发布的《个人信息出境安全评估办法（征求意见稿）》（“《2019 年办法（征求意见稿）》”，又针对个人信息的出境情形进行了更为明确的规范，但仍然保持着《2017 年办法（征求意见稿）》对整个网络运营者在境内收集的个人信息出境的规范立场。

《网络安全法》对于“网络运营者”的定义较为宽泛，包括了网络的所有者、网络的管理者、或者网络服务提供者三种角色。而无论是网络的所有者、管理者，还是任何使用网络收集、存储、传输、交换或通过网络处理消息以向最终用户提供产品和服务的企业都可能构成“网络运营者”。因此不难理解，在任何部门或行业中使用网络的任何位于中国境内的企业都有可能属于“网络运营者”，进而受到关于个人信息出境的规制。

作为“网络运营者”的企业在参与经济全球化的过程中，时常会涉及跨境传输个人信息的情形，因此，准确界定数据跨境传输行为是否属于个人信息出境，是企业在个人信息出境合规过程中最基础的一环。

《2019 年办法（征求意见稿）》将个人信息出境明确定义为网络运营者向境外提供在中华人民共和国境内运营中收集的个人信息的活动。《数据出境安全评估指南（征求意见稿）》第 3.7 条又提到，“数据未转移存储至本国以外的地方，但被境外的机构、组织、个人访问查看的（公开信息、网页访问除外）”的情形也属于数据出境。而 2020 年 10 月公布的《个保法草案》虽然没有对个人信息出境做出定义解释，但是针对个人信息跨境活动提出了专门的规定（请详见下文“二、个人信息出境的法律规范及责任” 中的相关内容）。

而从行业角度来看，我国部分领域针对特殊类别的个人信息也单独出台了法律条例或规定，对此类数据的出境进行了限制。具体而言：

1）.《征信业管理条例》第二十四条提出，“征信机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行”。

2）.《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》第六条指出，“在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息”。

3）.《网络预约出租汽车经营服务管理暂行办法》（2019 年修正）第二十七条提出，“网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于 2 年，除法律法规另有规定外，上述信息和数据不得外流”。

4）.《人类遗传资源管理暂行办法》第四条提出，“未经许可，任何单位和个人不得擅自采集、收集、买卖、出口、出境或以其他形式对外提供”重要遗传家系和特定地区遗传资源。

5）.《人口健康信息管理办法（试行）》第十条要求责任单位“不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器。”

6）.《国家健康医疗大数据标准、安全和服务管理办法（试行）》第三十条也指出，“健康医疗大数据应当存储在境内安全可信的服务器上，因业务需要确需向境外提供的，应当按照相关法律法规及有关要求进行安全评估审核。”

7）.《邮件快件实名收寄管理办法》第十六条则要求“寄递企业在中华人民共和国境内实名收寄活动中收集和产生的用户信息和重要数据应当在境内存储。”

8）.《证券基金经营机构信息技术管理办法》、《外商投资期货公司管理办法》、《私募投资基金服务业务管理办法（试行）》以及《关于加强在境外发行证券与上市相关保密和档案管理工作的规定》则对金融机构所涉及的客户信息及业务资料数据等做出了规范：除法律法规和中国证监会另有规定外，证券基金经

营机构不得允许或者配合其他机构、个人截取、留存客户信息，不得以任何方式向其他机构、个人提供客户信息。外商投资期货公司交易、结算、风险控制等信息系统的核心服务器以及记录、存储客户信息的数据设备，应当设置在中国境内。此外，在境外发行证券与上市过程中，提供相关证券服务的证券公司、证券服务机构在境内形成的工作底稿等档案应当存放在境内。

二、个人信息出境的法律规范及责任

正如上文所提到的，为避免个人信息出境对国家安全、经济发展、社会公共利益和个人合法利益带来风险，我国制定了一系列法律法规，旨在对个人信息出境做出限制。

值得一提的是，《个保法草案》第一次在法律层面 ，针对个人信息提出了系统性、全面性的保护要求，它借鉴了相关国家和地区的做法（如欧盟 GDPR），具有域外效力，明确在特定条件下，境外组织、个人在境外处理个人信息活动时，也适用该法。《个保法草案》第三条依托“属人原则”，着重对个人信息处理活动进行了规制。因此，一旦《个保法草案》在征求意见后正式出台，企业应关注其处理个人信息活动本身--是否具有向境内自然人“提供产品或者服务”的目的；是否存在分析、评估境内自然人的行为，从而判断该活动是否落入《个保法草案》的管辖范围。

具体而言，从跨境业务的角度出发，《个保法草案》针对的是“处理中国境内自然人个人信息的活动”，且在第三条第二款中特别规定，境内自然人进行数据分析、评估行为，应当落入《个保法草案》的管辖范围内。《个保法草案》对于境外企业处理境内自然人个人信息的行为也确认需进行规制和回应。比如，《个保法草案》第五十二条要求境外业务主体应在中国境内设立专门机构或指定代表，负责处理个人信息保护事务。若境外机构与境内机构共享信息，构成共同个人信息处理者的，还应当对个人信息主体共同承担义务和连带责任（《个保法草案》第二十一条）。此外，《个保法草案》第二十四条提出，若个人信息处理者向境内第三方提供个人信息时，除向个人履行相关告知义务外，还需要取得个人的单独同意。此种“单独同意”作为第一次出现在我国个人信息保护相关立法中的新概念，是否能够被目前惯常使用的通过隐私政策进行的“告知-同意”模式所覆盖，仍有待探讨，详细分析也可以参考本报告的其他章节。

根据现在已经出台或公布的《网络安全法》、《2017 年办法（征求意见稿）》、《2019 年办法（征求意见稿）》、《数据出境安全评估指南（征求意见稿）》、《国标》等法律及国家标准，同时结合《个保法草案》的内容，笔者认为目前对于个人信息出境提出的主要要求有以下三方面：（1）获得个人信息主体的授权同意；（2）确保数据输出方设立了专门机构或指定代表负责数据传输活动。；以及（3）达到监管部门的合规要求（比如通过个人信息安全影响评估等）。（请详见下文第三部分的内容）。

如果公司违反了上述规定，则会面临一定的法律责任。《网络安全法》规定，关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

此外，对于违反个人信息跨境提供的规则所应承担的法律责任，《个保法草案》未做出特别的规定，仅提出违反本法规定处理个人信息，将受到如由履行个人信息保护职责的部门责令改正，没收违法所得，给予警告；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。情节严重的，由履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款,并可以责令暂停相关业务、停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。可以看出，相较于《网络安全法》、《个保法草案》加大了惩罚力度。

值得注意的是，《个保法草案》第六十三条规定，有本法规定的违法行为的，将记入信用档案，并予以公示。笔者理解，对于特定行业的企业来讲，信用惩戒的后果包括限制申请主要业务的行政许可等，从而影响企业开展业务，这也将对企业产生严重的不利影响。

因此，为了保证出海业务的顺利进行，企业在个人信息出境前的规划中应当充分考虑出境的业务场景、出境个人信息类型以及各类个人信息在出境时是否会受到限制，以及违反相关规定应承受的法律责任等问题，避免在特定个人信息出境时遭遇阻碍、违反相关法律法规等情况，减少不必要的损失。

三、个人信息出境合规要点及建议

分析以上个人信息出境相关法律法规，笔者理解，企业在业务中涉及个人信息跨境传输的情况，应注重以下公司内部合规要点：

（一）个人信息主体的授权同意

个人信息出境需要遵循个人信息主体授权同意的基本性的原则。《网络安全法》规定，网络运营者在“使用”个人信息主体的个人信息，应当获得其授权同意。而“使用”包括“跨境传输”的行为，因此，对于未获得个人信息主体同意的数据，不得出境。《2017 年办法（征求意见稿）》进一步对此做出了明确解释，“个人信息出境，应向个人信息主体说明数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，并经其同意。未成年人个人信息出境须经其监护人同意。”此处的同意代指明示的同意，即需要个人信息主体通过书面、口头等方式主动做出纸质或电子形式的声明，或者自主做出肯定性动作，对其个人信息进行特定处理做出明确授权。《数据出境安全评估指南（征求意见稿）》也对于实践中构成有效同意的场景做出了列举，包括拨打国际及漫游电话、发送国际电子邮件、进行国际即时通信等。

《个保法草案》也提出个人信息处理者向中国境外提供个人信息的，应当向个人告知境外接收方的身份、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式等事项，并取得个人的单独同意，做出充分意思表达。

如果无法获得个人信息主体同意的，在某些特定场景（例如：危及公民生命财产安全等紧急情况的）下也可以将个人信息传输出境，但一般来讲这类种例外情形在企业的日常经营中发生的概率较小基本不会涉及，因此企业如需将个人信息传输出境的，征得个人信息主体同意仍是基础合规路径。

（二）设立专门机构或指定代表

为便于对境外个人信息处理者进行监管，《2019 年办法（征求意见稿）》规定境外机构经营活动中，通过互联网等收集境内用户个人信息，应当在境内通过法定代表人或者机构履行本办法中网络运营者的责任和义务。《个保法草案》参考 GDPR 规定，明确中国境外的个人信息处理者，应当在中国境内设立专门机构

或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。虽然草案未明确规定“个人信息保护职责的部门”具体指向，但此条款旨在保障草案域外管辖的可实施性，在发生个人信息安全风险时，使得相关监管部门能够在境内找到相应的主体，高效解决问题。

（三）达到监管部门的合规要求

对比《2019 年办法（征求意见稿）》、《个保法草案》明确了个人信息出境的限制，丰富了企业的跨境提供个人信息的合规场景，在实践中更具有可操作性。该法第三十八条明确，个人信息处理者因业务需要，向境外提供个人信息的企业应当至少具备下列一项条件：

1. 通过网信部门组织的安全评估

根据《2019 年办法（征求意见稿）》规定，省级网信部门的安全评估是个人信息出境的前置条件，一般网络运营者均应遵守。对于一般网络运营者对省级网信部门安全评估结论存在异议的，可以向国家网信部门提出申诉。

相较于此，《个保法草案》直接规定，关键信息基础设施运营者、处理个人信息达到国家网信部门规定数量的个人信息处理者向境外提供个人信息的，应当通过国家网信部门组织的安全评估。明确了此类期待更高安全等级的数据出境行为，应由国家网信部门统一进行安全评估。

因此，建议企业首先自查，其是否可能被视为关键信息基础设施运营者，或判断其处理个人信息的数量是否达到相关规定。并根据自身情况在进行个人信息出境之前事先对出境行为，参照省级和国家网信部门的安全评估标准，进行安全自评估，发现潜在风险并及时整改，以提高主管机关评估的通过率。

其中，企业应当重点评估以下内容：

1）.是否制定数据出境计划

2）.是否符合国家有关法律法规和政策规定。

3）.合同条款是否能够充分保障个人信息主体合法权益。

4）.合同能否得到有效执行。

5）.企业自身或接收者是否有损害个人信息主体合法权益的历史、是否发生过重大网络安全事件。

6）.企业获得个人信息是否合法、正当。

根据《2019 年办法（征求意见稿）》，如果个人信息被获准出境，企业应当建立个人信息出境记录并且至少保存 5 年。同时，企业应在每年 12 月 31 日前将本年度个人信息出境情况、合同履行情况等报所在地省级网信部门。

2. 经专业机构进行个人信息保护认证

正如本文第一部分第 12.2 节所述，《个保法草案》借鉴 GDPR 中关于 SCC、认证的相关规定，规定了专业机构进行个人信息保护认证，为企业数据进行正常商业贸易下的个人信息出境提供了更多选择和便利。除了单一申报网信部门进行安全评估，企业可以根据自身情况，按照国家网信部门的规定，选择专业机构进行个人信息保护认证。《个保法草案》对于专业机构未做出专门定义，有可能是中国网络安全审查技术与认证中心或者由个保法细则进行进一步指引，或在实践中探索相关规则。

3. 具备全面且完善的合同

除同意外，与个人信息接收方之间签署跨境传输协议应当是个人信息顺利出境的第二个核心要素。企业需要通过合同方式对接收方的权利和义务作出明确约定，就此保障个人信息的安全，维护个人信息主体及企业自身的合法权益。

首先，企业在合同中需要特别注意明确企业与接收方在本次合作中分别承担的角色，这不仅关系到后续数据安全事件中的责任分配，更是影响着企业制定内部政策及保护措施等重要环节。

企业与数据接收方之间既有可能是数据控制者与数据处理者的关系，也有可能是共同数据处理者的关系，需要根据具体的数据收集处理场景进行分析，并通过合同进行明确。根据《国标》第 3.4 条，个人信息控制者是“有能力决定个人信息处理目的、方式等的组织或个人”。因此，判断企业与数据接收者之间角色关系的核心要点在于，确认数据接收方对数据使用目的及方式是否拥有自主权。当

双方关系为“共同控制者”时，数据接收者对于数据的收集、使用等都拥有自决性，在获取后也无需要根据数据批露方的指令对数据进行销毁或者交还。一些数据接收方会出于后续业务发展、数据进一步变现的考虑，而自愿成为“共同数据控制者”的身份。因此，企业应考虑业务需求、具体出境的数据类型等，进行个案判断与评估。

在确定了双方分别承担的角色后，企业应当重点参考《2019 年办法（征求意见稿）》的具体规定，该办法除了要求企业在合同中明确个人信息出境的目的等基本情况外，还需要企业对个人信息主体的救济途径、接收方及批露方的责任义务、接收方所在国家的法律环境是否合适等诸多方面做出具体且明确的规定。企业在与境外接收方签署合同时，应当重点注意涉及上述规定的合同条款。

除此之外，《个保法草案》明确，企业应监督境外接收方在处理个人信息活动时是否达到了草案规定的个人信息保护标准，这实质上是为了保证落实《个保法草案》的域外效力。笔者理解，根据此规定，企业应该在订立合同前，确定数据接收方有能力达到《个保法草案》中有关个人信息保护的一般要求；在双方所订立的合同中，写明相关条款，明确接收方在合同履行过程中应当配合数据披露方的监督和指导，以符合草案的要求；在合同履行过程中，数据批露方企业应实时对标草案，监督数据接收方的行为，并确保满足草案的标准。

如个人信息主体有要求，企业还应当提供跨境传输合同的复印件，此合同也将作为监管机关进行安全评估的重点参考文件，建议企业提高对此类合同的重视程度并详细完善各项条款。

4. 主动报告并积极配合外部监管

《2019 年办法（征求意见稿）》将主要监管职责赋予省级网信部门，除了报请省级网信部门进行安全评估外，网络运营者应注意对于省级网信部门还有主动报告义务：

1）.应当于每年 12 月 31 日前，主动向所在地省级网信部门报送将本年度个人信息出境情况、合同履行情况等。

2）.发生较大数据安全事件时，应及时报所在地省级网信部门。

在做好企业内部合规的同时，企业应该积极配合有关部门的监管活动。一则，根据监管部门的要求，进一步自查并合规，维护良好的个人信息出境秩序，提前避免违法违规情况的发生；二则，在省级网信部门发现有损害个人信息主体合法权益、数据泄露安全事件等情况时，境内企业应按照其要求积极配合进行整改，并主动督促数据接收方进行整改。

企业在合规过程中除了应当注意以上要点以外，笔者建议企业还应当关注国家网信部门公布的限制或者禁止个人信息提供清单，提前采取措施，避免与清单中列名的组织或个人涉及跨境传输个人信息的活动。因《个保法草案》规定，境外的组织、个人从事损害中国公民的个人信息权益，或者危害中国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。虽对向以上清单中组织或个人跨境传输个人信息的行为，《个保法草案》暂未规定相应处罚措施，但如果企业跟清单中所列组织或个人达成合作协议，该合作涉及需要跨境传输个人信息的，而国家限制或禁止向该数据接收方提供个人信息的，将会影响双方合作，甚至产生纠纷，导致损失。

同时，当数据出境通过上述层层评估与审核，确认满足数据出境要求后，企业应注意这并非数据流转周期的终点。此时的合规应同时重点关注目标国家在个人信息与隐私保护领域的法律/法规、司法判例与合同要求，以确保数据在目标国家的保存、处理、共享、转让等符合相应的监管要求。具体可以参考由环球数据合规团队撰写的《数据全球化与隐私保护指引》。

四、结语

在数字经济与大数据的浪潮下，各国都在积极探索监管路径，以确保数据在实现其商业价值的同时不损害个人信息主体的各项权利。而美国虽然目前尚未在联邦层面制定统一的数据隐私保护法，但是已经通过在各个分散领域的法规中对某些特殊类型的信息及行业作出了针对性规定，单独针对个人信息与隐私保护的法案也已经在州层面已经开始推进和落实，如美国的《加利福尼亚州消费者隐私法案》（“CCPA”），通过消费者保护的角度对于个人信息的收集与处理做出规定，明确了数据保护规则和相关主体义务。而亚太地区各国家也都普遍重视个人信息保护与隐私安全问题并出台了相应的法案进行约束，如韩国的《个人信息保

护法案》（“PIPA”）、印度《个人数据保护法案》(“PDPB”)等。经过调研，笔者发现目前对于数据本地化要求更为严苛的有俄罗斯、伊朗、越南、塔吉克斯坦、多米尼加共和国等等，这些国家针对个人信息或某类特殊类别的数据具有明文的本地化要求。而其他大部分国家如欧盟地区、澳大利亚、巴西、加拿大、印度、日本、马来西亚、墨西哥、新西兰、菲律宾、沙特阿拉伯、新加坡、韩国、泰国等地，虽然有限制出境的规定在案，但是经过如监管机构的审批等前置程序后，是可以进行数据出境的处理活动的。

因此，笔者建议企业在进行数据出境及数据跨境传输活动之前，事先密切关注目标国家的个人信息保护法律法规与政策，并在数据出境后合法合规地完成后续处理流程，减少不必要的商业损失。

跨境商业活动日新月异，在中国个人信息出境相关法律法规正日趋完善的背景下，企业应当时刻关注立法动态，了解相关法律法规的规定及违反规定可能承担的法律责任。根据企业自身情况，在准确界定个人信息出境行为的基础上，切实做好企业数据合规方面的工作，减少在国际贸易中跨境传输个人信息违法违规的情形，避免受到监管机关的惩罚，保证商务活动顺利进行。

第五篇：个人信息保护工作机构及负责人设置要求

《个保法草案》第五十一条明确要求，处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。在法律层面明确了企业需要设立个人信息保护负责人这一要求，本文将重点介绍我国相关立法及标准的规定，并结合欧盟的要求进行比标分析。

一、欧盟

业内实践中，多以“DPO”作为此类岗位负责人的统一称谓。这一表述最初引自欧盟《通用数据保护条例》（GDPR）—“Data protection officer”。但是，GDPR 并未对其做出明确定义。笔者理解，DPO 集“普法专员”、“内部督查员”、“客服专员”、“政府公关专员”、“信息安全专员”等多岗位于一身，并具有独立履行职能，有助于企业遵守法律法规，引导企业和员工履行 GDPR 项下的义务，监督企业内部数据合规制度的执行，配合监管机构进行监督与执法，是“问责机制的基石与纽带”。

根据 GDPR 以及 EDPB 出具的相应解释条文，对于满足条件的企业，设立 DPO 属于一项必须履行的法律义务，尽管法规没有规定诸如“大规模系统监测”和“核心活动”等术语，但是，第 29 条工作组已就如何解释这些条款发布了指导原则。例如，社交媒体和搜索引擎公司作为数据控制者，其商业模式往往基于大量个人数据的处理、大规模定期和系统地监控数据主体，通过提供有针对性的广告服务和允许公司在其网站上订阅广告产生可观的收益。其中，效果类广告是一种根据人口统计数据和消费者历史购买记录或行为投放广告的方式，因此，需要系统地监控数据主体的在线习惯和行为。根据 GDPR，这类企业被强制要求任命 DPO。另外，医院和医疗保险公司的活动包括对特殊类别个人数据（包括遗传和生物特征数据）的大规模处理或披露，因此，同样需要加强保护，GDPR 也要求其指定数据保护官。如果不设立，属于违反 GDPR 的明确规定，将面临承担相应的法律责任。对于依法可以不设立 DPO 的企业，EDPB 的解释条文中仍建议这部分企业设立 DPO，并将 “是否有专人负责数据保护以确保组织按照 GDPR 的规定处理数据”作为证明公司合规性的有力参考因素之一。

在决定设立 DPO 后，企业接下来考虑的问题应当是 DPO 所应当具备的基本素质，从而缩小目标范围，确保委任的人选能够切实有效的帮助公司规避合规风险、及时响应监管及个人信息主体的要求并妥善处理。结合相关法律法规的要求，笔者认为，DPO 至少应当具备以下几点基本素养：

1）.掌握一定的专业知识并具有独立履行职责的能力，在处理数据保护方面有实践经验；

2）.与数据控制者之间有被雇佣或被委托的关系；

3）.具备较强的沟通与协调能力，能够妥善处理来自监管机构或个人信息主体的各项要求或投诉；

4）.熟悉公司内部的业务模式以及数据流转情况，能够对公司的合规工作提出可落地、可执行的建议措施。

而对于 DPO 的人选，公司既可以选择由公司内某位员工担任，也可以聘任外部人员如律师等担任。但考虑到 DPO 需要配合企业落实上文中所述的义务及要求，笔者建议企业在聘任 DPO 的时候优先考虑自有员工；如果公司出于其他考量需要从外部聘任 DPO 的，应当与其签订书面的聘用协议，并在协议中对 DPO 应当履行的职责及工作进行明确约定，从而确保 DPO 能够有效的帮助企业在业务正常发展的情况下满足法律监管的要求。

但需要提示公司注意，一旦公司任命了 DPO，必须确保其在所有与个人数据保护相关的问题中及时、全面地参与。为了使 DPO 能够有效地执行其任务，公司必须为其提供必要的资源，包括财务资源、基础设施和设备，还包括为 DPO 提供足够的时间来履行其职能，并提供持续培训，使他们能够发展自己的专业知识并及时了解数据保护法律法规的所有发展。此外，DPO 的成功设立，并不代表责任及义务的转移，数据控制者和数据处理者仍是承担责任的主体，在 GDPR 体系下，DPO 本人不会因为履行职责而受到免职或惩罚，WP29 更是明确地指出 DPO 对数据不合规不负个人责任，而是有数据控制者承担确保数据合规的义务。但 DPO 仍可能会因自身的渎职、失职行为而受到处罚，各成员国的立法中，部分国家也对 DPO 自身职责履行不当的情形做出了处罚规定。

因此，公司及 DPO 本人均应当充分重视：DPO 本人应当严格按法律法规履行职责，充分履行勤勉注意义务；公司应当给予充分的支持，并依照 DPO 的合规建议，在内部积极整改及落实。双方应当重点注意以下几个方面的合规义务：

1）.对现有法规进行解读、新法跟进以及定期组织法律法规内部培训；

2）.协助制定及落实符合法律法规要求的内部制度及流程等文件；

3）.负责开展及监督 DPIA 工作；

4）.对日常数据处理操作进行监督与审计，并提出合规意见；

5）.落实数据处理岗位相关员工的职责及义务说明；

6）.在监管机关审查时，履行配合、响应义务；

7）.DPO 直接向最高管理层报告，其履行的其他任务或职务不能与 DPO 的职务产生利益冲突。

如果企业未按上文规定设立 DPO，且又属于应当设立 DPO 的情形，根据 GDPR 相关规定，可能会面临高达 2000 万欧元或者前一财年全球收入的 4%的罚款。而在 DPO 的责任承担方面，如上文所述，GDPR 也明确禁止 DPO 因为履行职责而被免职或惩罚，此外，为确保 DPO 能够独立且高效的履行或行使上述的义务或权利，GDPR 还提供了一些基本保证。例如，控制者和处理者必须确保在执行与数据保护相关的任务时，DPO 不会受到公司（包括最高管理层人员）的任何干扰性指示。此外，不得因他们执行任务而以任何方式解雇或处罚他们。例如，DPO 认为，组织的活动可能会导致数据主体处于高风险，建议数据控制者或者处理者进行数据保护影响评估。如果公司不同意 DPO 的建议，不认为它有充分根据并决定不进行安全影响评估的，公司可以忽略这些建议，但是，不能因 DPO 提出了建议而解雇或惩罚他/她。

DPO 能否有效开展后续的合规工作，更多情况下取决于企业领导层的支持与配合。同理，企业负责人对个人信息安全内容的熟识程度与支持力度，也取决于 DPO 平时对政策动态、行业资讯的及时了解并主动分享和与企业负责人进行沟通交流。DPO 与公司之间多是一种互相支持与促进的关系。企业任命 DPO，并给予

相应的资源支持，DPO 则应为企业的业务发展保驾护航。定期组织全员培训，提高员工的数据保护意识，能够有效避免安全事件、用户投诉等问题发生。

企业设立 DPO 除了可以落实这一项法定义务外，还可以在 DPO 的协助下从上文所述的几个方面提升合规水平，成本与收益的对比一目了然。

二、中国

相较于欧盟以统一、集中且具体的方式对 DPO 的设立及职责等情况进行规定，我国目前没有“DPO”或“数据保护官”这一称谓。但是，可以从一些现行法律法规及国家标准中找到类似的表述。从实质看，这些职务尽管叫法不同，其设立的目的与意义都是类似的，以下可能统称为“数据保护岗位负责人”。

笔者对目前各法律法规及标准中对类似职位的名称职位、职责以及未设立相应职位可能受到的处罚情况进行简要汇总与对比。

法规	职务名称	职责	未设立的法律后果
《网络安全法》	网络安全负责人	落实网络安全保护的相关工作。	一百万元以下的罚款及警告、责令改正的处罚。
《银行业金融机构数据治理指引》	首席数据官（自愿）	主要负责人对数据质量承担最终责任。	/
《儿童个人信息网络保护规定》	儿童个人信息保护负责人	负责儿童个人信息保护相关的工作，对内部员工处理儿童个人信息的行为采取审批、记录等限制措施。	参照《网络安全法》的规定，推定可能会受到 10 万元以下的罚款及警告、责令改正的处罚。
《个保法草案》	个人信息保护负责人	对个人信息处理活动以及采取的保护措施等进行监督。 个人信息处理者应当公开个人信息保护负责人的姓名、联系方式等，并报送履行个人信息保护职责的部门。	五千万元以下或者上一年度营业额百分之五以下罚款及警告、没收违法所得、责令暂停相关业务、停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照的处罚。

《关键信息基础设施保护条例（征求意见稿）》	关键信息基础设施网络安全管理负责人	1）组织制定网络安全规章制度、操作规程并监督执行； 2）组织对关键岗位人员的技能考核； 3）组织制定并实施本单位网络安全教育和培训计划； 4）组织开展网络安全检查和应急演练，应对处置网络安全事件； 5）按规定向国家有关部门报告网络安全重要事项、事件。	一百万元以下的罚款及警告、责令改正的处罚。
《国标》	个人信息保护负责人	1）全面统筹实施组织内部的个人信息安全工作，对个人信息安全负直接责任； 2）组织制定个人信息保护工作计划并督促落实； 3）制定、签发、实施、定期更新个人信息保护政策和相关规程； 4）建立、维护和更新组织所持有的个人信息清单（包括个人信息的类型、数量、来源、接收方等）和授权访问策略； 5）开展个人信息安全影响评估，提出个人信息保护的对策建议，督促整改安全隐患； 6）组织开展个人信息安全培训； 7）在产品或服务上线发布前进行检测，避免未知的个人信息收集、使用、共享等处理行为； 8）公布投诉、举报方式等信息并及时受理投诉举报； 9）进行安全审计； 10）与监督、管理部门保持沟通，通报或报告个人信息保护和事件处置等情况。	/

1. 设立与职责

从上表可以看出，关于数据保护岗位的设立和职责的规定，我国多是以“一般+特例”的方式进行规定，至于这几个岗位之间的关系，笔者主要从上表所列的职责范围以及各职位之间能否兼任这两个维度进行具体分析：

1）.职责范围

结合法律法规及项目工作经验，笔者对上表中各职位的职责范围进行比对，仅供公司在设立相应职位时参考。

首席数据官≥网络安全负责人=网络安全管理负责人>个人信息保护负责人>儿童个人信息保护负责人。

2）.兼任情况

《国标》中明确规定对于满足一定条件[31]的企业，应当设立专职人员负责个人信息保护工作。除此之外，我国现阶段没有其他关于上述岗位必须由专职人员担任的规定。

- 在排除法律法规的禁止性规定后，从岗位本身的职责范围判断，笔者认为，“首席数据官”、“网络安全负责人”及“网络安全管理负责人”（如果某企业同时还是关键信息基础设施运营者的情况下）三个职位基本可以由同一人兼任的，而“个人信息保护负责人”的职责范围相比较之下则更特定更具体，建议有个人信息保护方面实践经验与专业知识的人员担任则会更好，因为在一定程度上可能还有与消费者、监管机构沟通的需求。基于企业运营合理性的考虑，在职位委任方面，笔者将针对企业规模与发展阶段的不同情况，给出如下参考性建议：

- 如果企业属于初创类型公司，所涉及的数据量级及业务体量等情况不具备设立个人信息保护负责人条件的，可以由网络安全负责人或者信息安全负责人或者法务负责人兼任。

[31] 《国标》第 11.1 条（c）规定，满足以下条件之一的组织，应设立专职的个人信息保护负责人和个人信息保护 工作机构，负责个人信息安全工作： 1) 主要业务涉及个人信息处理，且从业人员规模大于 200 人； 2) 处理超过 100 万人的个人信息，或预计在 12 个月内处理超过 100 万人的个人 信息； 3) 处理超过 10 万人的个人敏感信息的。

- 如果企业的规模已经符合《国标》中规定的需要设立个人信息保护负责人的情况，建议可以由不同的员工分别担任网络安全负责人（偏信息安全）和个人信息保护负责人（偏隐私安全）。当然，如果网络安全负责人同时也兼具有个人信息保护知识与经验的，也可以由同一人担任两个角色，并且给予“数据保护官”的专门职务。待企业规模再大时，甚至还可以给该人配置专员，以共同支持网络安全与个人信息保护的全盘工作，或者由其他岗位的同事一起成立个人信息与隐私保护委员会。

- 如果企业涉及的个人信息处理活动频繁且信息量级较大，但企业规模又不足以设立专职的个人信息保护负责人的，建议可以在网络安全负责人下由一名员工专项负责个人信息保护工作，例如：互联网公司、广告公司、大数据企业等。

- 如果企业主要的经营活动基本不涉及个人信息处理相关的工作，更多涉及网络运营维护、网络安全技术等方面的事项，但偶尔也有可能接触到客户或员工的个人信息，可以由一人同时兼任网络安全负责人和个人信息保护负责人。例如：网络技术服务公司等。

针对儿童个人信息保护负责人，笔者认为，如果公司主营产品的直接或间接受众是儿童，且有条件设立儿童个人信息保护专员的，建议除设立个人信息保护负责人外，还应委任专人担任儿童个人信息保护负责人。反之，可以由个人信息保护负责人兼任，因为除了儿童群体特殊，有专门保护要求以外，其保护的对象均是个人信息与隐私安全。如果企业所售产品或者提供服务并非特别针对儿童，覆盖的是全年龄段的用户，则可以直接由个人信息保护负责人来兼任儿童个人信息保护负责人的角色。对于完全不从事收集、存储、使用、转移、披露儿童个人信息等活动的企业，可以不设立此职位。

综上所述仅是笔者结合法律要求及实践经验给出的建议，部分法律法规均处于草案、征求意见稿阶段，各职位间的兼容性还有待于法律法规的进一步解释。

2. 法律责任

通过上文表格可以看出，现阶段对于企业未设立数据保护岗位负责人有处罚的生效法律依据主要源于《网络安全法》、《儿童个人信息网络保护规定》。但随着后续《个人信息保护法》的正式出台及实施，对于未设立个人信息保护负责

人的企业，可能会面临非常严重的处罚后果。因此，建议企业可以参考《个保法草案》以及《国标》中的相关规定，及早设立个人信息保护负责人，以避免在发生数据泄露等事故时，经监管审查发现没有设立个人信息保护负责人，而被依据生效后的《个人信息保护法》进行处罚。

在责任承担的主体方面，不同于 GDPR，我国法律法规并没有对个人信息保护负责人的责任豁免作出任何直接明确的规定，也没有直接规定个人信息保护负责人在哪些情形下会承担法律责任，鉴于个人信息保护负责人属于在企业内部主持数据安全与与个人信息保护工作的人，不能排除其属于“直接负责的主管人员以及其他责任人员”，如因自身工作存在故意或过失，或从事违法行为，有可能需要承担相应的民事、行政甚至刑事责任。

但从笔者对法条及目前执法案例、司法判例的理解，个人信息保护负责人在尽到了合理、谨慎、注意义务且自身不存在任何违法行为，如数据保护岗位负责人尽职尽责，已对所有发现的风险进行了披露并且反复要求企业进行整改，而企业仍然置若罔闻，不予理睬的，那么大多数情况下，个人信息保护负责人不应当再承担法律责任了，但企业自身仍是对外承担安全责任的主体。

3. 实务建议

结合上文对中欧数据保护岗位负责人应当承担的责任义务的分析与对比，下文将对我国企业数据保护岗位负责人如何开展工作及履行职责，提供一些参考性的建议。

1）.基础工作的铺垫

在企业内部的合规工作，首先是让管理层明晰合规工作的重要性。数据保护岗位负责人可以将发生的数据相关案例处罚原因、处罚情况以及后续影响进行汇总并汇报给管理层，这样容易引起重视。其次，建立数据安全保护小组或虚拟委员会。依照目前国内的情况看，除了部分企业设有数据保护专职岗位以外，大多数企业是由信息安全或者法律合规部门来兼顾处理数据合规事务。但是，合规工作不仅仅涉及信息安全或法律问题，还需要考虑产品经营模式、消费者投诉、技术手段等多方面内容。建立数据安全保护小组或虚拟委员会，让不同部门的人更深入了解企业内部各方的工作，有助于协调统一地推进工作。最后，对所做的一

切合规工作（如评估报告、内部培训等）都需要有留存记录（即留痕），证明企业为数据合规已经开展了实质性工作，也是日后监管机构来核查时的主要参考依据。

2）.组成机构的职责分配

一般情况下，法律合规部门、数据运营部门、各产品线、运维和 IT 部门与个人信息安全保护工作最密切相关，因此，可以由其中一个部门的负责人牵头（如果符合条件，亦可被委任为数据保护岗位负责人），从相关部门抽取核心人员（经签署专项保密协议后）共同组建企业个人信息保护工作机构，各司其职，分别负责《国标》要求的各项具体内容。具体说，包括以下几个方面：

由法律合规部负责制定、签发、实施、定期更新隐私政策和相关规程；组织开展个人信息安全培训；制定应急预案和组织应急演练；对滥用个人信息的投诉、举报进行调查，严厉查处不合规现象和违纪员工，如非授权访问、篡改或删除个人信息，违规使用、滥用信息等；维护企业个人信息保护的联系途径，对个人信息主体提出的疑问或投诉进行解答与处理；对机构内部各部门的执行情况进行审计，包括对隐私政策的落实情况、对安全事件的处置、应急响应和安全能力审计等，如有需要，还应当与相关监管机构保护日常良好的沟通。

由法律合规部牵头，数据运营部门及其他必要部门配合组织开展个人信息安全影响评估，包括个人信息收集和使用的评估，并形成评估报告（每年至少一次）；建立、维护和更新个人信息清单（包括个人信息的类型、数量、来源、接收方等）和授权访问策略；对用户发布的信息进行管理，对特殊信息进行报告。

由产品经理对用户隐私政策结合产品进行发布；对弹窗式等通知以及权限管理等问题进行产品设计；对个人信息主体要求访问、更正、删除、撤销同意等请求进行产品可实现性支持；预设个人信息泄露时的通知机制；在产品或服务上线发布前进行检测，避免未知的个人信息收集、使用、共享等处理行为。

由运维部门对个人信息存储及每次流转进行安全影响评估，形成相应的评估报告；制定数据本地化存储的管理制度，梳理与第三方企业的安全保障责任和义务，对日志留存、数据分类、备份和加密等进行管理。

由 IT 部门负责对企业整体网络环境进行事先评估，制订相关信息安全、网络

安全，以及信息、网络的应急管理制度，负责网络的运行管理：安全配置网络参数，严格控制网络用户访问权限，维护网络安全正常运行；监控网络关键设备、网络端口、网络物理线路，防范黑客入侵，及时向个人信息保护工作机构报告安全事件，对有安全隐患、缺陷和漏洞的网络进行及时修补，制定补救机制。

3）.建设企业数据合规体系

建设完备的数据合规体系是一项大工程，建议国内数据保护岗位负责人重点从以下三个层面开展数据合规或治理工作：第一，梳理数据流转情况。需要清楚、全面地了解企业内部对数据收集、使用、共享、转让、公开披露、存储、删除等环节的现状以及所有配套机制的实施情况，比对相关法律法规及标准后，对不足部分进行改进；第二，完善内部制度规程。主要包括设置访问权限控制机制、建立个人信息安全影响评估制度以及采取技术保护手段等；第三，完善外部文件，包括用户协议、隐私政策以及与第三方签订的合同等。外部文件是外部评估企业合规水平的重要参考依据，最好结合之前对数据流转情况的梳理完成。第四，需要有对危机事件做出迅速反应、评估与决策，安排并分配处理信息安全事件相关人员，对事件采取措施并向监管机构进行报告，与投诉/举报人和媒体进行充分沟通的能力；第五，在合适时机将企业内部合规能力与成绩对外进行展示。

当前，很多企业的业务模式不仅仅局限于国内。因此，在完成上述工作后，数据保护岗位负责人还需要考虑如何在国内与国外不同的监管模式下创设符合公司实际情况的合规路径。数据保护岗位负责人首先需要考虑国内对于数据出境的要求。具体要求与适用的法律法规依据，请参考本报告第一和第二部分中涉及到数据出境相关内容的详细分析与建议。无论企业进行至少每年一次的自评估还是需要报请相关主管部门组织评估，组织进行安全评估已经成为数据出境的前置程序。数据保护岗位负责人需要对这些程序非常了解或者咨询专业机构的意见。其次，要兼顾目标国家的相关法律要求。如果企业拥有出海业务，数据保护岗位负责人需要知悉并结合各个目标国家的不同隐私保护规定，制定出与出海目标国家相配套的合规方案。具体建议，请参考环球数据合规团队撰写的《数据全球化与隐私保护指引》。最后，从节约成本与提高效率为出发点，根据企业实际情况，是考虑选择创设多法域的不同合规路径，还是采用“统一 + 特殊”的路径，这些都需要数据保护岗位负责人帮助企业完成选择并拟定有效措施。

三、结语

随着《个保法草案》的发布，企业设立个人信息保护负责人已经同 GDPR 一样成为了法定义务而不是建议性的规定，但无论是 GDPR 规定的 DPO 制度，还是我国的网络安全负责人/个人信息保护负责人制度，其角色定位的核心均是提前防治企业运营中可能遇到的安全风险。究其根本，是人们对个人信息保护的逐渐重视与意识的不断提升。数据资产将最终成为企业的核心竞争力，做好数据合规不仅仅对企业自身的业务运营有极大的帮助，在企业进行融资、并购、上市等过程中，也已经成为了投资人衡量企业价值的核心要素。企业在保障数据合法合规处理的同时，最好还能够建立起自身的合规文化，将数据保护意识贯彻在日常工作中，并将其形成常态。而这一切工作的开端，大都需要数据保护岗位负责人的牵头、推动并争取到全公司上下各方面的支持与配合。

环 球 律 师 事 务 所
GLOBAL LAW OFFICE

Global Law Office | 环球律师事务所

www.glo.com.cn

北京市朝阳区建国路81号华贸中心
1号写字楼15层&20层
邮编: 100025
15 & 20/F Tower 1,
China Central Place,
No. 81 Jianguo Road, Chaoyang
District, Beijing 100025, China
电话/T. (86 10) 6584 6688
传真/F. (86 10) 6584 6666

上海市徐汇区淮海中路999号
环贸广场办公楼一期35层&36层
邮编: 200031
35 & 36/F
Shanghai One ICC, No. 999
Middle Huai Hai Road, Xuhui District,
Shanghai 200031, China
电话/T. (86 21) 2310 8288
传真/F. (86 21) 2310 8299

深圳市南山区深南大道9668号
华润置地大厦B座27层
邮编: 518052
27/F Tower B,
China Resources Land Building,
No. 9668 Shennan Avenue, Nanshan
District, Shenzhen 518052, China
电话/T. (86 755) 8388 5988
传真/F. (86 755) 8388 5987

成都市高新区天府大道北段966号
天府国际金融中心11号楼37层
邮编: 610041
37/F Building 11,
Tianfu International Finance Center,
No. 966 Tianfu Avenue North Section,
High-tech Zone, Chengdu 610041, China
电话/T. (86 28) 8605 9898
传真/F. (86 28) 8313 5533