全球数据保护政策

前言

CORNING[1] 是特殊玻璃和陶瓷材料领域的世界领先者。我们开发并生产用于消费性电子产品、移动排放控制、通信和生命科学领域的高技术系统的关键部件。开展业务时，我们会收集和处理有关公司员工、求职者、临时工、客户、供应商及其他业务合作伙伴的相关个人数据[2]。

现行政策（以下称为“政策”）阐明了 CORNING 就个人数据保护做出的承诺。为了确保提供最大程度的个人数据保护，CORNING 遵循欧盟法规 2016/679 中关于保护自然人的个人数据处理以及自由迁移该等数据的标准（以下称为“通用数据保护条例”或“GDPR”）。

此外，CORNING 实施了一套公司绑定规则（“BCR”），以确保在 CORNING 集团内传输个人数据时提供保护。BCR 的实施为位于欧盟的 CORNING 实体向位于全球各地的其他 CORNING 实体传输个人数据提供充分的保护[3]。BCR 的原则与 GDPR 一致。BCR 不仅能够使集团内的国际间个人数据传输合法化，还可确保 CORNING 一致而有效地遵守全球各地的数据保护法规。CORNING 在全球范围内对所有个人数据处理采用 BCR。想要了解更多关于 BCR 的信息，请访问 http://www.corning.com/worldwide/en/privacy-policy/binding-corporate-rules.html

CORNING 还设立了隐私办公室（以下称为“Corning 隐私办公室”或“CPO”），努力通过采用数据保护政策与程序、员工培训以及定期监控是否满足数据保护标准的计划来促进 CORNING 遵守全球数据保护规定。

CORNING 努力使所有数据主体都能轻松获取现行政策。为此，CORNING 内网和 CORNING 外部网站都发布有此政策的当前版本。

I. 本政策的目的

本政策的目的：

i. 阐明 CORNING 在处理个人数据时采用的标准。
ii. 说明 CORNING 集团就个人数据保护采取的管理行动。
iii. 概述个人数据得到处理的数据主体享有的权利，以及其他们如何行使这些权利。

II. 政策范围

本政策适用于[4]由任何 CORNING 实体或代表任何 CORNING 实体对所有个人数据进行的处理，不论该等个人数据采用何种格式（例如电子档案、纸质档案、录像等）。

CORNING 实体及所有 CORNING 员工、临时工都必须遵守本政策。除 GCPR 以外，每个 CORNING 实体还应遵守适用的地方数据保护要求。

此外，由 CORNING 委托或代表 CORNING 委托处理个人数据的所有供应商[5]与所有适用的第三方[6]必须就个人数据保护标准提供符合要求的保证，此类保证至少应等同于本政策所包含之保证。

---

[1] “CORNING”（或“我们”）是指总部位于美国纽约州科宁的 Corning Incorporated（一家纽约公司），以及由 Corning Incorporated 直接或间接拥有或控制的全球子公司。如本文所用，拥有或控制一家实体需要直接或间接持有该实体的股份或其他权益，并在选举或任命该实体的董事、管理人员、普通合伙人或类似职位时，拥有超过百分之五十（50%）的表决权或其他类似权力。在下文中，该集团企业有时也被称为“CORNING 集团”。

[2] “个人数据”是指与指定自然人或可识别自然人（“数据主体”）有关的任何信息；可识别个人是指其身份可通过参考身份证号码，或特定于该人员身体、生理、心理、经济、文化或社会身份的一个或多个因素，直接或间接地识别出来的人员。在保护与指定或可识别的法律实体有关信息的适用国家数据保护法允许的范围内，术语“个人数据”也应包含此类信息。

[3] “数据传输”是指从一个实体向另一个实体传输任何个人数据。个人数据的传输可通过网络，以通信、复制、传输或泄露的形式进行，包括远程访问数据库或在任何类型的介质之间传输（无论介质类型为何，例如从计算机硬盘传输到服务器）。

[4] “处理”是指对个人数据执行的任何自动或非自动操作，例如收集、记录、组织、构造、存储、改编或更改、检索、咨询、使用、传输泄露、散布或以其他方式提供、排列或组合、限制、擦除或损毁。

III. 一般规则

CORNING 致力于根据 BCR 和本政策中规定的原则，保护和保障由员工、求职者、临时工、客户、供应商、业务合作伙伴及其他相关人员委托给 Corning 的个人数据。

CORNING 的数据保护实践和计划符合 CORNING 的价值观和适用的法律法规。对于委托给供应商和业务合作伙伴的个人数据，CORNING 要求供应商和业务合作伙伴采取严格程度至少与 CORNING BCR 中所述程度相当的数据保护实践。

IV. 数据保护原则

处理个人数据的法律依据

CORNING 仅在以下情况收集和处理个人数据：

- 资料当事人已同意[7]就一个或多个特定目的处理其个人数据；或
- 为履行资料当事人签署之合约，或为了在签订合约之前应资料当事人要求采取措施，而必须处理个人数据；或
- 为遵守 CORNING 的法律义务而必须处理个人数据；或
- 为保护资料当事人或其他自然人的切身利益而必须处理个人数据；或
- 出于公众利益而执行任务，或为行使 CORNING 或向其泄露个人数据的第三方的职务权限，而必须处理个人数据；或
- 为追求 CORNING 作为管理者或[8]向其泄露个人数据的第三方的合法权益，而必须处理个人数据，除非资料当事人需要受到保护的基本权利和自由比此类权益更为重要（尤其当资料当事人为儿童时）。

处理特殊类别的个人数据的法律依据[9]

CORNING 不会处理特殊类型的个人数据，除非：

- 资料当事人明确同意处理此类个人数据（适用的法律明确禁止的情况除外）；或
- 为履行 CORNING 实体依据雇佣法作为管理者的义务和行使特定权利，而必须进行处理，这些义务和权利由欧盟或国家法律或规定采取充分保护措施的集体协议授予；或
- 为保护资料当事人或因资料当事人身体或法律原因而无法表示同意时其他人的切身利益而必须进行处理；或
- 为确立、行使或捍卫合法求偿权而必须处理个人数据；或
- 资料当事人明确公开的特殊类别的个人数据的相关处理；或
- 出于重大公众利益而必须进行处理；
- 为评估员工工作能力而必须进行处理；
- 出于公众利益、科学或历史研究或者统计目的（依据 GDPR 第 89 条规定）而必须进行处理。

CORNING 可能会处理与犯罪、刑事定罪或安全措施有关的个人数据，在这种情况下，此类个人数据处理只能在官方机构的控制下执行（若适用），并且必须采取适用国家法律规定的具体保障措施。此外，地方数据保护法律可对国家身份证号码的处理进行具体限制。

目的限制

---

[5] “供应商”是指 Corning 采用的指代其大多数处理方的术语。供应商为按 Corning 指示处理个人数据的签约实体，例如工资单提供商。

[6] “第三方”是指自然人或法人、公共机关、机构或组织，但资料当事人、管理者、处理方以及受管理者或处理方直接领导并经授权处理数据的其他人员除外。

[7] 本政策中未另行定义的所有大写术语均具有 GDPR 所规定的含义。

[8] “管理者”是指单独或与其他方共同决定个人数据处理之目的和方式的自然人或法人、公共机关、机构或任何其他主体。

[9] “特殊类别的个人数据”是指透露种族或民族、政治观点、宗教或哲学信仰、工会会员资格、遗传数据、生物特征数据、健康相关数据、自然人的性生活或性取向相关数据的个人数据。

CORNING 出于指定、明确和合法的目的处理个人数据，不会以不符合此类目的的方式做进一步处理。CORNING 在以下情况下不会进一步处理个人数据：未核实是否获得资料当事人的事先同意；处理是否基于法律义务；或数据处理的新目的是否与最初收集和处理数据的目的一致。

数据质量与最小化

CORNING 在合法商业利益要求的范围内，同时考虑个人的权利，以公正合法的方式收集和处理个人数据。

CORNING 只出于合理必要的商业目的收集个人数据。在处理个人数据时，CORNING 确保仅收集和/或进一步处理相关且适量的数据，不会超过此类目的的范围。为特定目的收集的个人数据的具体类型可能各不相同，主要取决于收集的原因和适用的法规。如果 CORNING 收到的个人数据超出收集的预期目的或与之无关，或超出向资料当事人提供的信息范畴，CORNING 应酌情采取措施，以防发送人进一步传输过多或无关的个人数据，并且应使用合理的方式（例如销毁）确保不会进一步处理无关或过多的个人数据。

准确性和时效性

CORNING 采取适当的措施以确保处理的个人数据准确无误，并且在必要时对其进行更正和更新。就数据收集或进一步处理目的而言，CORNING 应在适当时采取措施，确保擦除或更正不准确或不完整的个人数据。资料当事人可以联系以下相关章节中指定的 CORNING 联系点。如果可能，CORNING 还会向个人提供自助式访问、更正和/或更新其个人数据的途径。

适当的数据保留

CORNING 采用允许进行识别的方式保留满足法律和商业保留要求的个人数据，并且不存储与收集和处理数据的目的不再相关的个人数据。在以下情况，CORNING 会采取合理的措施来销毁个人数据：(i) 就资料收集目的而言已不再需要，和/或 (ii) 已超过适用法律（如有）规定的最长保留期限。

自动个人决策

CORNING 采取适当的措施以确保每一位资料当事人有权不接受对其带来法律效果或产生重大影响以及仅基于自动个人数据处理而做出的决策，包括旨在适用的数据保护条例规定的条件下对该资料当事人的某些个人方面进行评估的说明（例如，除非该决策对由该资料当事人与 CORNING 订立或履行合同而言是必须的，或该决策由 CORNING 遵循的适用数据保护法律许可或已获得资料当事人的明确同意）。

透明度和知情权

根据透明度原则，Corning 确保向资料当事人提供的信息明了且资料当事人可获取该等信息。该等信息采用方便获取的形式和清楚易懂的语言呈现。

CORNING 至少向资料当事人提供以下信息，除非资料当事人已经获得该等消息：

- 管理者的管理者代表（如有）的身份和联系方式，适当情况下还包括管理者在 EEA 以外的办公场所；
- 数据保护主管（根据 GDPR 或其他适用的欧盟数据保护法律酌情指定）的联系方式；
- 处理个人数据的目的以及法律依据；
- 若基于合法权益进行处理，管理者或第三方所追求的合法权益
- 个人数据的接收者[10]接收者类别；适当情况下，向第三国传输个人数据，以及相关保障的详细信息，包括欧盟委员会是否做出充分性决策，以及获取个人数据的方式或将个人数据提供给谁
- 任何其他信息，例如：
    - 存储个人数据的时间段，如果没有该信息，则为用于确定该时间段的标准；

[10] “接收者”是指接收泄露数据的自然人或法人、公共机关、机构或任何其他组织，无论其是否为第三方；然而，在特定调查框架内接收数据的机构不应被视为接收者。

- 提供个人数据是法律要求还是合同要求，资料当事人是否有义务提供个人数据以及未提供该等数据可能带来的后果；
- 做出自动个人决策（若有），包括说明，包括关于所涉及的逻辑相关的有意义信息以及为资料当事人处理数据的意义和潜在后果；
- 要求管理者访问、更正或删除个人数据或限制处理资料当事人的相关信息或者反对处理的权利，以及移植个人数据的权利；
- 如果在同意有权随时撤销该同意的情况下进行处理，在其撤销同意之前，不对数据处理的合法性产生影响；
- 若违反数据保护法规，有权向监管当局投诉[11]。

此外，根据 Corning 依据 BCR 做出的承诺，在此信息声明中，Corning 也将通知资料当事人该资料当事人是否遭受处理其个人数据相关的任何损害，该资料当事人有权获得赔偿，并且在适当的时候将获得管辖法院或监管当局所判决的或依据内部 Corning 投诉机制（若使用）所确定的赔偿（参见 BCR 的第 5.4、6.3 与 6.4 条规定以了解具体权利。

如果资料当事人未直接获取个人数据，CORNING 也将向该资料当事人提供相关类别的个人数据和个人数据来源相关的信息，在适当情况下还包括该信息是否来自公众可获取的来源。在这种情况下，上述信息将在以下情况下提供：

a. 在获取个人数据后的一段合理时间内提供，但最迟在一个月内提供，会考虑处理个人数据的具体环境；
b. 如果个人数据被用于与资料当事人交流，最迟在第一次与资料当事人交流时提供；或
c. 如果计划向第三方泄露，最迟在第一次泄露个人数据时提供。

通知资料当事人的义务在以下情况下不适用：(i) 资料当事人已掌握该信息；或 (ii) 其与付出的努力不成比例，或 (iii) 管理者遵循的法律明确要求记录或泄露该等个人数据并且提供适当的措施来保护资料当事人的正当权益；或(iv) 根据欧盟或国家法律规定的职业性秘密义务（包括法定保密义务），个人数据仍然必须保密。

访问、更正、删除、限制处理的权利，以及反对处理或数据移植的权利

CORNING 采取充分的手段以接收资料当事人对其权利提出的要求并予以回复。

每个资料当事人都有权：

- 在合理的时间间隔内，在不受限制、无过度迟延或过高费用的情况下，适用时根据国家法律从 CORNING 获得相关信息：
  - 确认是否正在处理与资料当事人相关的个人数据，
  - 如果是，至少为数据处理的目的、相关数据的类别以及个人数据的接收者或接收者类别；若可能，则为存储个人数据的计划时间段，若不可能，则为用于确定该时间段的标准、拥有要求 CORNING 更正或删除个人数据或限制处理资料当事人的相关个人数据或反对该等处理的权利、向监管当局投诉的权利、以及就其来源而言的任何可用信息（并非从资料当事人处收集个人信息的情况）；进行自动化决策，包括说明以及至少为所涉及的逻辑相关的有意义信息以及为资料当事人处理数据的意义和潜在后果；
  - 若向第三国传输个人数据[12]，为传输所采取的适当保障措施的相关信息；以简洁明了的形式向资料当事人传达正在处理的个人数据以及其来源相关的任何可用信息；
- 及时从 CORNING 获取信息，更正并删除关于其的不准确个人信息，删除个人数据或限制个人数据的处理；
- 行使自己的数据移植权利，从 CORNING 获取接收关于其的个人数据的权利，个人以结构化的通用机器可读格式向 CORNING 提供个人数据；

[11] “监管当局”是指负责以下方面的独立主体：(i) 监管辖区内的个人数据处理监控，(ii) 向主管机构提供有关个人数据处理方面的立法和行政措施建议，以及 (iii) 听取资料当事人提出的有关其个人数据保护权利方面的投诉。

[12] **“第三国”**是指欧洲经济区（EEA）之外的国家。

- 以资料当事人面临的特殊情况相关的正当合法理由，随时拒绝个人数据处理（当处理是基于 CORNING 的合法权益时）；
- 无需声明合法理由，在处理数据期间的任何时间反对出于直接营销目的（包括与该等直接营销相关的说明）而进行的个人数据处理。

针对向资料当事人提供访问、更正和删除 CORNING 维护的关于他们的个人数据的权利，以及提供拒绝个人数据处理、获得限制处理或获得数据可移植性的权利，CORNING 制定了相关程序，用于说明角色和职责。

资料当事人可将请求提交至 privacy@corning.com，或通过邮件、亲自递送、电话或电子邮件提交给指定数据保护主管（“ADPO”）或地方隐私联系人（“LPC”）或其他业务职能代表。

为了使得 CORNING 能够回复所有请求，资料当事人必须向 CORNING 提交以下必要的身份数据：名字、姓氏、电子邮件或通讯地址以及为确定其身份所需的任何其他必要信息。

CORNING 可拒绝过分的请求，尤其是在数量、重复性或系统性特征方面过分的请求。

投诉的权利 如果资料当事人怀疑 Corning 不遵守适用的个人数据保护法规，则资料当事人亦有权向监管当局投诉。

安全性和保密性

考虑到技术发展水平和实施成本，CORNING 实施了从商业角度来看合理的适当技术与组织方面安全措施，以对其收集和持有的个人数据进行保密，同时保护这些数据不会受到未经授权或非法的泄露或访问、意外丢失、销毁、更改或损坏。这些措施旨在针对受保护之个人数据性质上与处理中的固有风险，提供程度与适用的数据保护法规定之安全要求一致的适当安全保护。

CORNING 采取了适当的措施，以确保被授权访问个人数据的供应商应采取至少与 CORNING 所实施安全措施同样严格的安全措施。

个人数据违规通知

在特定环境下，应向主管监管机构和受影响的资料当事人通知个人数据违规行为[13]。

CORNING 确保采用充分的手段来履行该义务。具体地讲，CORNING 员工应向 privacy@corning.com或相关 ADPO 或 LPC 报告任何可疑或实际的个人数据违规行为（包括包含个人数据的设备丢失或损坏）。Corning 隐私办公室将与其他相关 Corning 利益相关者一起及时处理个人数据违规行为。

Corning 集团内部或外部的个人数据传输

CORNING 是一家全球化企业，在全球各地设有法人实体，其业务、IT 系统、管理结构和流程均跨越国界。因此，CORNING 经常需要将个人数据传输到与最初提供该个人数据的一方位于相同或不同国家/地区的其他 CORNING 实体、供应商或第三方，和/或将个人数据存储到在其他国家/地区托管的数据库或可从其他国家/地区访问的数据库。CORNING 采用的 BCR 系统具有符合欧盟法律规定的原则、规则和工具，可确保有效的数据保护级别，尤其是在向欧洲经济区（EEA）以外的 CORNING 实体传输个人数据时。更明确地说：

- 传输到 CORNING 实体：只有在个人数据的传输是基于合法的具体商业目的，并且接收实体保证遵守本政策、BCR，以及适用于数据传输和后续处理（包括前向传输）的更严格的任何地方法律的情况下，才可在 CORNING 实体之间传输个人数据。根据 BCR 规定，如果一家 CORNING 实体要求另一家 CORNING 实体代表其处理个人数据，接受处理服务的 CORNING 实体应选择另一家就规管数据处理的技术与组织方面安全措施提供充分保证并且确保遵守这些措施的 CORNING 实体。受 BCR 约束的 CORNING 实体承诺提供充分的保证，并且在代表另一家

[13] “个人数据违规”是指违反安全规定，导致有意或非法销毁、丢失、更改、未经授权泄露或访问所传输、存储或处理的个人数据。

CORNING 实体作为处理方[14]时遵守 BCR 包含的所有保障措施，尤其是要遵守 CORNING 实体对传输个人数据及实施技术与组织方面安全措施的指示，以通过具体的数据处理协议充分保护个人数据不受意外或非法损坏或意外丢失、更改、未经授权的泄露或访问。此外，如果在作为联合管理者的两家 CORNING 实体之间传输数据[15]，应签订书面协议，规定各自的责任以遵守 GDPR 下的义务，尤其是涉及到行使资料当事人的权利时。

- 向 CORNING 集团外的实体传输数据：

- 供应商：CORNING 已经或将要与供应商签署书面合约，以确保供应商根据 CORNING 的指示处理个人数据，建立和维护适当的安全和保密措施，提供适当水平的保护。此外，CORNING 还要求此类供应商就以下方面提供符合要求的保证：(i) 其标准至少与本政策所含的标准相当；(ii) 遵守适用的数据保护法，尤其是适用于个人数据传输和前向传输的法律。此类供应商只在出于执行适用服务合约中规定的服务时，才可访问个人数据。如果 CORNING 实体认为供应商未遵守这些义务，将立即采取适当的措施。此外，CORNING 不会向欧盟外的供应商传输个人数据，除非此类供应商根据相关欧盟隐私权要求采用适当的隐私和安全控制措施以保护个人数据（例如，如果供应商所在的国家/地区不提供充分的个人数据保护，则确保供应商签署欧盟委员会批准的欧盟标准合同条款）。此外，对于联合管理者之间的关系（若有），Corning 应与遵守 GDPR 的任何外部联合管理者签订书面协议。

- 第三方：CORNING 实体可能需要向第三方泄露特定个人数据。尤其是在为了遵守适用的法律（例如向税务局泄露薪资数据）或在资料当事人的健康或安全受到威胁（例如发生事故）时，可能需要进行此类泄露。CORNING 还可能出于保护其合法权利（例如在诉讼中）的目的泄露个人数据。

责任

为了证实自己遵守本政策规定的原则，CORNING 实施了以下措施：

i) 记录处理行为

CORNING 对涉及个人数据的处理行为保留内部记录[16]。这些记录必须提供给任何主管监管当局以用于调查目的。

ii) 有意设计和默认提供的数据保护

CORNING 必须采取专门设计的适当技术与组织方面措施，以有效实施数据保护原则，并且在数据处理中整合必要的保障措施，从而在确定处理手段和处理本身的时间点时满足数据保护要求并保护资料当事人的权利。

此外，CORNING 必须采取适当的技术与组织方面措施，以确保在默认情况下仅处理对出于每个具体目的而言必要的个人数据。此规则适用于所收集的个人数据量、该等数据的存储时间以及可访问性。

iii) 数据保护影响评估

当数据处理可能对资料当事人的权利和自由带来较大风险时，CORNING 将执行数据保护影响评估（即 DPIA）[17]。DPIA 对处理行为进行评估，以确定数据处理可能对资料当事人的权利和自由带来的影响并且就管理该等影响提出建议。

V. 对于遵守本政策的承诺和实施方式

[14] “处理方”是指代表管理者处理个人数据的自然人或法人、公共机关、机构或任何其他组织。
[15] 两位或多位管理者共同确定数据处理的目的和手段。
[16] 参见 GDPR 第 30 条规定。
[17] GDPR 的第 35 条规定。

CORNING 设立了 CORNING 隐私办公室（“CPO”），其成员包括全球首席隐私官（“GCPO”）、地区数据隐私经理、指定数据保护主管（若 GDPR 和/或适用的数据保护法律有此要求）和地方隐私联系人。CPO 负责管理 CORNING 集团层面本政策和 BCR 的遵守情况，同时发起并协调有关本政策、BCR、相关政策及程序的完善事宜。CORNING 也对各种计划进行维护，以定期监控本政策的遵守情况，帮助确保 CORNING 实体、员工遵守适用于个人数据处理的 BCR、相关法律、要求及合约协议。

此类计划包括定期培训和审计，确保 CORNING 能够验证政策和 BCR 的准确性、完整性、突出显示性、完全实施性和可访问性。

Corning 实施了培训计划以增强员工对数据保护问题的意识。收集、处理或访问个人数据的新员工及临时工需要完成数据保护培训计划。此外，收集、处理或访问个人数据的所有员工均应定期完成此类计划。

此外，内外部团队将定期执行数据保护合规审查，以确保本政策、BCR 以及所有其他相关政策、程序或指南得到更新和应用。

VI. 索赔处理与执行机制

如果以违反本政策或 BCR 的方式访问、处理或使用个人数据，CORNING 实体将根据适用的法律采取适当的补救措施，其中可能包括纪律处分。

如果资料当事人认为，对其个人数据的处理方式违反了本政策或 BCR，资料当事人可以按如下所述方式提起投诉。

针对处理资料当事人所提起的数据保护投诉以及对于数据保护投诉的接收、记录、调查与回复，CORNING 制定了相关程序，用于说明相关角色和职责。

Corning. com 拥有方便资料当事人提起投诉的实用工具，包括以下至少一项：

- 投诉表的网络链接，
- 电子邮件地址、电话号码或通讯地址。

员工提交的数据保护投诉

CORNING 员工可通过 CORNING 内网和外部 CORNING 网站上的数据保护投诉表提交数据保护投诉。填写完数据保护投诉表后，可通过以下方式提交：

- 发送电子邮件至 CPO 的邮箱，邮箱地址为：privacy@corning.com
- 通过电子邮件、邮寄或亲自递送的方式提交给指定数据保护主管或地方隐私联系人或人力资源、销售、营销、全球供应管理、财务、健康和安全部门以及任何其他必要的业务职能部门。

其他资料当事人（例如临时工、供应商、客户）提交的数据保护投诉

其他资料当事人可通过 CORNING 对外网站上的数据保护投诉表提交数据保护投诉。填写完数据保护投诉表后，可通过以下方式提交：

- 通过电子邮件、邮寄或亲自递送的方式提交给指定数据保护主管或地方隐私联系人、客户服务代表、GSM 代表或销售及营销代表。
- 发送电子邮件至 CPO 的邮箱，邮箱地址为：privacy@corning.com

登记完投诉后，该投诉将在合理的时间内确认并处理（例如，在收到请求后一个月内，考虑到请求的复杂性和数量，在必要时可能再延长两个月）。CORNING 将通知资料当事人所延长的时间（若适用）。

如果资料当事人对 Corning 的回复不满意或资料当事人倾向于绕开可用的内部投诉机制，资料当事人有权向相关监管当局投诉[18]和/或在主管司法管辖区内寻求援助[19]。

[18] 如果 GDPR 适用，则在资料当事人的惯常居所或工作所在地或涉嫌侵权地的欧盟成员国内。
[19] 若 GDPR 适用，则为本地数据管理者有营业机构或资料当事人有惯常居所的成员国的法庭。

VII. CORNING 联系点

如果您对于本政策有任何疑问，或需要进行投诉或提出请求（例如访问、反对或更正请求），建议您通过以下信息联系 CPO：

Corning Privacy Office
One Riverfront Plaza
MP-HQ-E1-B23A
Corning, NY 14831
(607) 974-9000

Privacy@corning.com

如果您是 CORNING 员工，还可联系当地或部门的指定数据保护主管（若有）、地方隐私联系人或人力资源指定联系人。

VIII. 修订

本政策可能会不定期修订。最新版的政策将于 Corning 内网和外部网站上发布，也可能在适当的时间以硬拷贝或电子版形式发给所有员工。