Graphic Packaging INTERNATIONAL	**参考：** CI- XX
全球隐私政策 公司指示	**最近一次发布日期：** 2024 年 3 月 1 日 **重新发布日期：** XX – XX - XXXX **生效日期：** 2024 年 3 月 1 日

目录

政策声明

Graphic Packaging 致力于保护员工和客户的个人数据。为确保透明度及遵守全球隐私法律，本隐私政策概述：

- Graphic Packaging 收集的个人数据类型；
- Graphic Packaging 为什么收集这些个人数据；
- 如何使用和处理个人数据；
- 关于个人数据的权利和选择；
- 保护个人数据法；以及
- 与隐私相关的当局联系人。

范围

本《政策》适用于全球所有 Graphic Packaging 人员、地点和其他资产，其中包括但不限于：

- 所有 Graphic Packaging 业务单位、部门和职能团队；
- 所有 Graphic Packaging 承包商、顾问和其他第三方服务提供商，除非是在指明面向员工的具体要求的情况下；
- Graphic Packaging 业务运营时所在的 Graphic Packaging 租赁或自有的所有设施；以及
- 所有 Graphic Packaging 技术和网络基础设施，其中包括其信息系统、应用程序、系统平台和 Graphic Packaging 正常运营中所进行的计算机操作。

此处引用或链接的某些政策是内部政策，仅供指定员工使用。如果您是员工且无法访问某项链接政策，请联系 law.department@graphicpkg.com 获取副本。

关键术语

"数据主体"是指其个人数据已经或正在被处理的自然人。

"个人数据"包括与已识别或可识别的自然人有关的所有信息，例如员工的姓名和雇佣记录、客户代表的姓名和业务联系方式、供应商代表的姓名和业务联系方式，以及与我们网站访问者在我们网站上的浏览偏好有关的数据。

"处理"是一个非常宽泛的术语，本质上是指对个人数据或用个人数据做的任何事情（包括简单地收集、存储、访问或删除个人数据）。

个人数据处理

Graphic Packaging 致力于进行透明的个人数据处理实践。将通过清晰简明的隐私声明和同意机制，向个人告知收集了哪些个人数据、为什么收集这些数据，以及如何使用这些数据。个人数据只能出于特定、明确、合法的目的而收集，不得违背此类预期目的进行进一步处理。只有在个人同意或法律允许的情况下，才允许变更目的。

Graphic Packaging 仅收集实现我们声明的目的所必需的个人数据，并避免收集过多或不相关的信息。数据收集流程将包括适当的安全措施，以保护数据免受未经授权的访问、披露、更改和破坏。

数据最小化、设计隐私和敏感度降低

保护个人隐私的最佳方式之一就是首先不要收集他（她）的个人数据。对 Graphic Packaging 所持有的人数据进行处理，必须是预期目的真正需要的；我们将只收集完成该处理目的所需的最低数量。换句话说，我们绝不会收集我们不需要的个人数据。

在设计隐私和默认隐私原则的基础上以实现新的应用程序，服务和产品，这也是 Graphic Packaging 的明确目标。设计隐私意味着必须从任何系统、服务、产品、功能或流程的开始以及整个生命周期都考虑隐私，这需要积极参与技术创新、规划和设计阶段的风险识别和缓解，以及持续的审查和重新评估。默认情况下，隐私意味着我们组织中的每个 IT 系统、服务、产品或业务实践都被配置为保护个人数据。这意味着数据主体不需要执行任何额外的措施来保护他们的隐私，并且适用系统中的默认设置应该默认设置为最具保护性。

Graphic Packaging 通过尽可能降低所存储信息的敏感度，进一步最大限度地降低数据暴露的风险；具体方法是：

- 降低收集后所保留数据的精度。例如，如果客户电话号码用于统计分析，将只保留数字的子集，如区号。
- 将个人数据转换为不太敏感的形式。例如，当使用客户的 IP 地址来确定位置以进行统计分析时，该 IP 地址将在映射到城市或城镇后被丢弃。
- 限制对大量个人数据的访问。例如，需要访问个人数据的个人记录的员工不会自动拥有访问批量个人数据的权限。

维护处理记录

某些法律和法规要求 Graphic Packaging 为个人数据的使用、存储和处理方式保持准确记录（这些处理记录和创建这些记录的过程也称为数据映射）。除其他事项外，对处理活动的记录必须包括我们处理的个人数据的类别、我们使用的相关供应商和服务提供商的列表、我们使用个人数据的目的以及此类个人数据在国外的任何传输（例如传给位于外国的供应商）。数据映射是欧盟和英国“一般数据保护规定”(GDPR) 的基本义务。美国某些州的隐私法通常还要求 Graphic Packaging 等组织能够证明其是如何使用个人数据的，而数据映射练习可以轻松满足这一要求。Graphic Packaging 致力于维护准确、最新、全面的数据映射。

数据保护影响评估 (DPIA) 和风险

Graphic Packaging 的隐私管理计划旨在控制和减轻隐私风险。隐私风险侧重于 Graphic Packaging 处理的个人数据对个人的影响。这是 Graphic Packaging 更大的商业风险评估的一部分。

为了在需要的司法管辖区实现透明和控制，Graphic Packaging 会进行隐私影响评估 (PIA) 或数据保护影响评估 (DPIA)。当 Graphic Packaging 政策要求时，或者法律或合规要求时，作为项目日历准入要求清单的一部分进行 PIA 或 DPIA。

术语 PIA 和 DPIA 经常互换使用，但通常 DPIA 指的是欧盟和英国 GDPR 下的特定法律义务，而 PIA 通常指的是根据另一项隐私法或作为隐私计划最佳实践进行的一般隐私风险评估。在 Graphic Packaging，我们使用术语 PIA 来指代在 OneTrust 合规门户中执行的初始风险评估，评估结果决定是否必须进行全面的 DPIA。

进行 DPIA 并不是 Graphic Packaging 可能承担的所有项目的强制性要求。每当一个项目可能对个人的权利和自由造成高风险时，特别是在使用新技术的情况下，法律要求进行 DPIA。

因此，DPIA 本质上是一种风险评估，必须考虑个人数据处理的性质、范围、背景和目的，并且必须在开始处理之前进行该评估。无论特定的 Graphic Packaging 项目是内部的，还是由第三方提供的流程、产品或系统，DPIA 都应在项目的采购或设计中尽可能早地开始，即使某些项目操作仍不确定。

更多信息请参见 Graphic Packaging 的 ***DPIA 政策和程序***，详见此处：隐私影响评估政策。

处理个人数据的法律依据

只有在 Graphic Packaging 有有效合法依据的情况下，才允许处理个人数据。处理个人数据有多个可用的合法依据。在开始任何处理活动之前，我们必须确定将要使用的合法依据，这一点很重要。

我们的隐私声明将规定出于特定目的处理个人数据的合法依据。Graphic Packaging 还应记录我们所做出的决定（合法依据适用于特定处理活动），从而证明遵从适用的数据隐私法律法规。

处理个人数据的典型合法依据包括：

- 同意：当个人（数据主体）明确同意出于特定目的处理其个人数据时。同意应以书面或其他法律允许的方式宣布，必须事先告知个人处理个人数据的目的以及任何可能的传输。当同意声明作为其他声明的一部分时，必须突出显示，以便对于个人是清楚的。
- 合同：当 Graphic Packaging 已与另一个组织或个人所达成合同而必须进行处理时。
- 法律义务：当 Graphic Packaging 遵守法律而必须处理个人数据时（这不包括合同义务）。
- 合法利益：当出于 Graphic Packaging 的合法利益或第三方的合法利益而必须处理个人数据时，除非有充分理由保护个人的个人数据，而这些理由超越了这些合法利益。

数据安全

保密和授权

只有有义务遵守数据保密要求的 Graphic Packaging 经授权员工才被允许参与个人数据处理。禁止他们将此类个人数据用于个人目的、将个人数据转移给未经授权的方面或者以任何其他不正当方式让未经授权的人访问这些数据。

在此语境内，“未经授权”包括员工在不履行其员工职责的情况下对个人数据进行的任何访问或其他使用。保密义务在雇佣关系终止后仍然有效。

加密和假名化

在可能的情况下，在与预期保护目的相关的成本合理的情况下，在早期阶段使用个人数据匿名化或假名化。启用假名化是通过平衡的度量集来实现的，其中包括屏蔽（静态和/或动态）、令牌化和/或加密。

定期安全审计和测试

Graphic Packaging 定期进行安全审计和评估，以识别漏洞、评估风险以及加强安全措施。执行渗透测试和漏洞扫描是为了主动识别和解决潜在的安全弱点。有关详细信息，请参见审计及合规评估政策，详见此处：审计及合规评估政策

监控

Graphic Packaging 保留在法律允许的情况下监控电子邮件和网络流量的权利。其他详细信息，请参见可接受资产使用政策，详见此处：可接受资产使用政策

社交媒体

Graphic Packaging 认可员工参与社交媒体活动。Graphic Packaging 保留在法律允许的情况下监控社交媒体活动的权利，但也将尽可能努力保护员工的隐私。详细信息请参见 Graphic Packaging 的社交网络可接受使用政策，详见此处：社交网络可接受使用政策

移动设备管理 (MDM)

Graphic Packaging 的员工使用智能手机和平板电脑等移动设备。Graphic Packaging 在可能的情况下，在允许出于个人原因使用这些设备的情况下，将努力保护个人数据。详细信息请参见以下政策：

- **资产管理政策**，详见此处：资产管理政策
- **移动计算安全政策**，详见此处：移动计算安全政策
- **个人拥有设备政策**，详见此处：个人拥有设备政策

数据保留

个人数据保留的时间越长，意外泄露、丢失、被盗和/或信息变得陈旧的可能性就越大。换句话说，时间是数据泄露的关键促成因素。在 Graphic Packaging，目标是仅在支持业务目的或满足法律要求所需的最短时间内保留个人数据。

Graphic Packaging 保存的任何个人数据都受记录管理计划的管理，该计划规定数据保存的时间和原因，以及从所有数据存储中删除数据的方式。

更多信息请参见 Graphic Packaging 的记录管理计划政策，详见此处：记录管理计划政策

数据主体权利

Graphic Packaging 致力于维护数据保护和隐私方面的最高标准。作为我们对透明度和问责制承诺的一个组成部分，Graphic Packaging 遵守、承认并尊重适用的数据保护法律法规中概述的数据主体权利。

特殊类别和敏感个人数据

特殊类别的个人数据可能包括揭示种族血统、性取向、政治观点、宗教或哲学信仰、公民身份和移民身份、工会会员身份的信息，以及有关健康或性生活的数据。此类敏感个人信息由适用的当地数据隐私法界定并根据其进行处理。

考虑到语境和属性、数量和预期用途，在评估隐私风险后，在 Graphic Packaging 进行的个人数据的其他处理活动也可能被视为敏感活动。例如，Graphic Packaging 的薪资管理语境中的财务信息需要额外的保护和安全管控。

有关数据分类的更多信息，请参见信息分类政策，详见此处：信息分类政策

数据共享和第三方

Graphic Packaging 可能决定与第三方签订合同，收集、存储或处理数据，其中包括个人数据。第三方可能提供托管、外包、私有或公共云计算服务等服务。

如果 Graphic Packaging 决定与第三方签订处理个人数据的合同，在执行任何合同之前，必须由 IT 项目管理办公室 (PMO) 进行审查。在批准第三方进行处理时，与第三方的关系必须由书面协议加以规范，其中明确 Graphic Packaging 和分包商的权利和义务。应选择一个分包商，该分包商将保证本隐私政策中要求的技术和组织安全措施，并在保护个人数据和行使数据主体权利方面提供充分保证。

分包商必须根据合同义务仅在合同范围内以及 Graphic Packaging 发布的指示内处理个人数据。任何涉及个人数据处理的合同都必须附有法务部批准的数据保护附录。不得为任何其他目的而进行个人数据处理。Graphic Packaging 仍然对合同合作伙伴处理的个人数据负责。

数据泄露通知

防止个人数据泄露是所有 Graphic Packaging 员工和合同工的责任。此外，如果个人数据处理活动出现违规情况，我们鼓励每个人通知负责隐私事务的法律顾问，或在某些地区通知数据隐私官。

与及时发现、响应、处理和通知（监管机构和潜在的受影响的个人）有关的政策在 Graphic Packaging 的数据泄露响应政策中有所概述，详见此处：数据泄露响应政策以及安全事件响应政策，详见此处：安全事件响应政策

国际数据传输

在组织内外进行的个人数据传输是借助批准的协议和安全渠道安全地完成的。Graphic Packaging 遵守国际数据传输方面的相关法律法规要求，并确保在国际传输个人数据之前使用正确有效的数据传输机制。其中包括确保 Graphic Packaging 与所有可能代表 Graphic Packaging 处理个人数据的第三方供应商和服务提供商签订符合适用数据保护法律法规的合同。

遵守法律法规

Graphic Packaging 遵守管理个人数据处理和保护的相关国际、国家和地方法律法规，其实包括但不限于欧盟 GDPR、英国 GDPR、巴西一般数据保护法以及美国联邦和州隐私法。

培训、提高认识和强制执行

Graphic Packaging 将确保本隐私政策中规定的一般原则得到遵守。在这方面，Graphic Packaging 的管理人员应确保本政策得到实施，其中特别包括向员工提供政策信息。

员工还需要确认他们理解并承诺遵守本隐私政策。

如果需要额外培训，应向隐私委员会提出请求。政策信息还应包括提醒：在某些情况下，违反本隐私政策的一般原则可能会导致法律后果，如刑事处罚、责任和雇佣后果。

数据保护官 (DPO)

Graphic Packaging 已任命一位全球 DPO 来监督和确保遵守数据保护法律法规。在适用或必要的情况下，Graphic Packaging 还指定一位当地 DPO 来满足当地的合规要求。已提供 DPO 的联系信息（包括全名、职位和联系方式），供个人就任何数据保护问题、疑问或请求进行联系。DPO 与管理层、员工和相关利益相关方合作，以确保在整个组织中采用全面的数据保护方法，并作为 Graphic Packaging 数据保护问询的联系点。

版本控制

日期	变更描述	作者
XX	XX	XX