PUBLIC

ROQUETTE
Offering the best of nature™

Privacy & Data Protection

我们每天如何贯彻隐私和数据保护

隐私和数据保护

《良好行为指南》

罗盖特集团

法务与合规部门

罗盖特合规性关键挑战

在综合管理层的领导下，罗盖特的合规范围及其管理是集团“法务与合规部门”的一个关键部分，被称为合规办公室。

合规办公室负责罗盖特《行为守则》及其更新和实施。

该办公室还涵盖以下两个主要领域：

- 财务安全；
- 职业道德与；
- 隐私和数据保护。

因此，已制定并正在完善一项合规计划，以确保我们的业务在法律和财务方面没有纰漏。

合规性的作用是什么？

合规性的作用是灌输**道德价值观**并根据**法律要求**、**标准**及**良好做法**采取措施。

我们的计划促进了各项程序的实施，确保符合罗盖特适用规定。

我们的四项价值观——**真诚**、**卓越**、**前瞻**、**关爱**——构成了我们**日常**行事的坚实基础。

请谨记，当今时代，遵守道德规范的企业才是可持续发展的企业。

而公开透明的公司才是拥有明天的公司。

放眼全球

立足本地

卷首语

我们《行为守则》中规定的各项标准包含隐私和数据保护原则。

所有各位，包括与罗盖特有着关联的第三方，都拥有隐私权。罗盖特也因此致力于保护他们的个人数据。

个人数据，是可直接或间接用以识别自然人的信息（姓名、出生日期、社会保障号码、照片、电子邮件地址、计算机 ID 等）。

个人数据保护是确保隐私的一项基本权利

个人数据的保护，让每个人对这些数据的收集、处理、使用和分发享有控制支配权。

个人数据在用于明确、特定的合法用途时必须公平地使用，而且只能在数据处理的必要时期保存。

在欧洲，《通用数据保护条例》（GDPR）已对个人数据处理做出规定，该条例于 2018 年 5 月 25 日生效。

各国有关隐私和个人数据的法律各不相同，而作为国际化企业的罗盖特集团，已采用了有关个人数据保护的集团政策。该政策适用于集团全球所有员工。

本指南说明了我们在日常活动中应遵循的良好行为，从而符合个人数据保护原则及该政策的要求。

数据保护官员**珍妮佛 • 戈丁（Jennifer GODIN）**

Déléguée à la protection des données

目录

目标

什么是《隐私和数据保护政策》？

罗盖特集团已制定了一项《隐私和数据保护政策》（《政策》），从而根据集团形象和利益以及适用的法律法规进行数据保护，以最好的方式解决隐私和数据保护问题。

该《政策》规定了个人信息保护的各项原则和要求，并提出了罗盖特所有员工、经理、董事及第三方在隐私和数据保护方面应遵守的各项规定。

一个文档平台详述了该《个人数据保护政策》的各项原则和规定，包括三个级别：

- 管理承诺：《行为守则》
- 内部规定：Q-Docs 中的《个人数据保护手册和指令》。
- 数据保护管理系统（DPMS）文档：程序、准则、方法、学习等。

所有文档均符合数据保护法律法规要求。

什么是《隐私和数据保护良好行为指南》？

《隐私和数据保护指南》（《指南》）有助于我们实施并遵守我们的隐私和数据保护政策。

《指南》以浅显易懂的方式介绍了数据保护方面的各项规定和最佳做法，从而符合我们集团指令以及适用的法律法规要求。

《指南》包括与《行为守则》相对应的各项主题，其中“隐私和数据保护”属于合规性方面的一个话题。

说明

《隐私和数据保护良好行为指南》的适用对象？

《政策》和《指南》是全球范围内所有实体的共同基础。它们适用于：

- 所有员工、董事和经理（“员工”）
- 代表罗盖特的任何第三方，如：
  - 承包商，包括顾问、自由职业者和临时员工
  - 培训生
  - 来自非罗盖特实体的借调人员
  - 散工
  - 其他代表
  - 以及罗盖特雇用或向其付费的任何第三方。

我们可以在哪里找到《隐私和数据保护良好行为指南》？

所有代表罗盖特的员工和第三方都必须理解并遵守公司文档——尤其是本《指南》——中包含的隐私和数据保护原则。

《指南》即将在 ONE 门户上发布：

全球职能部门 > 数据保护 > 良好行为指南。

本《指南》作为沟通专题的一部分进行传播，并附有工具包及有关隐私和数据保护原则（根据国际标准和《通用数据保护条例》的具体要求而规定）的电子学习课程。

该培训课程包含在“数据保护新手引导计划”中。

责任

谁负责实施操作原则？

在我们的组织中，数据隐私关乎人人，人人有责。

我们所有人都有责任遵守合规办公室团队和数据保护网络提供的 DPMS 文档中描述的操作原则。本《指南》有助于实施的开展，并提高我们的合规水平。

我们怎样才能确保自己做出正确的决定？

《指南》旨在帮助我们处理工作生活中可能产生隐私问题的大多数情况。但是，它无法预见我们在开展职业活动时可能遇到的每一种情况。

如果我们在任何时候对采取何种态度有任何疑问，我们必须运用良好的判断力并自问以下问题：

- 这合法吗？
- 这能够很好地体现我自己和公司吗？
- 我会将此事告诉朋友、家人或同事吗？
- 假使这事公开的话，我会感到舒服吗？

如果这些问题中有任何一个的答案是“否”，我们就不应该继续。如果我们有任何疑问，我们应该与集团数据保护官或其他相关人员联系（请参阅“提出问题或疑虑”部分中的联系信息）。

如果我们不遵守隐私和数据保护原则会怎样？

不遵守这些原则会对公司产生不利影响。对于公司和相关个人而言，后果可能非常严重（纪律处分、罚款、监禁、损害声誉等）。

所有关于已证实的或可疑的违规行为的报告都将被认真对待。我们将根据法律要求及时公平地进行调查。

按照数据泄漏的性质，可能会根据当地法律和公司规章采取纪律处分措施。

在任何一项调查中，所有员工都必须充分合作。罗盖特将保护牵涉其中的任一人员的隐私。

提出问题或疑虑

鼓励员工、代表罗盖特的第三方及其他利益相关者提出可帮助罗盖特防止并减少对公司造成伤害的问题或疑虑。

可以提出什么样的问题？

可以提出任何问题以及违反隐私和数据保护原则、公司法规或适用法律的任何潜在或实际违规行为。

我们应该联系谁？

如发生数据泄露，请联系数据保护官（dpo@Roquette.com ）和/或通过我们的网络表格 "Privacy Alert "报告事件。

如果您需要报告潜在的违规行为，可以与您的常规联系人联系，或通过 Speakup© 设备报告问题。通过该设备收到的所有警报都会得到保密处理，并遵守相关法律法规。

SpeakUp

罗盖特绝不容忍对善意举报违反隐私和数据保护原则或适用法律的潜在或实际行为的员工或第三方进行任何形式的报复。

因此，如果业务违规行为的举报者必须表明身份时，则组织必须对其身份进行保密处理，以避免因举报而遭受报复、歧视或纪律处分的危险。

遵守法律法规

在集团各个实体中的我们每个人，都应遵守现行数据保护法律法规。

如果当地法规比我们的《政策》和《指南》要求更严格，则以前者为准。

否则（没有地方法规或法规要求不严时），在法律允许的范围内，以我们的内部良好做法为准。

我们认为：

- 我们必须尽快实施所有新的本地适用法规。
- 我们每个人都必须意识到，任何违反法律法规的行为都可能会对涉及其中的个人及公司造成民事和/或刑事制裁。
- 在个人数据处理方面保护自然人是一项基本权利。
- 无论国籍或居住地如何，在个人数据方面处理保护自然人的原则和规定均应尊重其基本权利和自由，特别是其个人数据保护的权利。
- 个人数据保护的权利并非绝对权利；必须根据比例原则，考虑该项权利在社会中的作用，并与其他基本权利保持均衡。

哪个国家已通过了具体的数据保护法规或设立了数据保护机关？

请查阅该地图了解概况：https://www.cnil.fr/en/data-protection-around-the-world。

我们的责任：

- 在任何情况下，我们都必须遵守数据主体所在国家所有适用的数据保护法律法规以及公司各个所在地的所有现行规定。

- 作为业务活动的一部分，我们应将自己认为违反适用数据保护法律法规（如《通用数据保护条例》）的任何行为举报至数据保护官：dpo@Roquette.com，和保密的 Roquette 警报装置： Speakup©.

- 我们必须制定与环境相适应并相称的个人数据保护措施，同时加强遵守其他法律法规。反过来，我们遵守适用于本集团的法律法规的行为必须符合个人数据保护的规定和良好做法（例如：在“反贿赂和腐败”合规计划中，我们必须通过保密措施保护举报人并保护其个人数据）。

您是否受《通用数据保护条例》（GDPR）的约束？

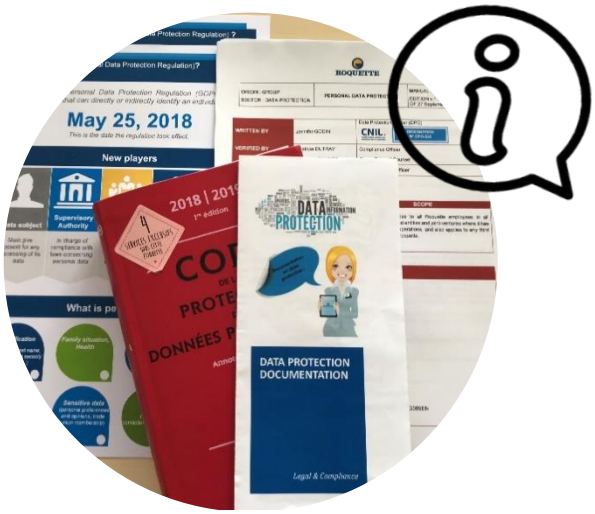
在以下情形中，您作为数据**处理方**[1]或**控制方**[2]受《通用数据保护条例》的管辖：

- 如果公司是在欧盟境内成立，或；
- 当公司并不是在欧盟境内成立时，则如果：公司的“数据处理活动涉及
  - 向欧盟境内的数据主体提供商品或服务；
  - 对其发生在欧盟境内的行为的监控”。

官方案文：《通用数据保护条例》第 3 条有关“地域范围”的规定

（1）和（2）：请参阅第 38 页的定义。

数据 保护原则



个人数据必须：

- 安全。
- 准确，及时更新。
- 公平合法地进行处理。
- 出于限定用途而进行处理。
- 充分、相关、不过度。
- 在限定且确定的期限内保留。
- 根据数据主体的权利进行处理。
- 在传输到其他国家时受到适当法律措施的保护。

您的权利：

根据适用的法律法规，您有权出于正当理由访问、纠正您的数据以及反对对您的数据进行处理，还有权出于正当理由擦除数据，并拥有数据可移植性的权利和限制处理您数据的权利。

如要行使这些权利，请填写以下网页中的表格：Roquette.com/Data Protection。

如有任何要求，请联系**数据保护官**（dpo@Roquette.com）。

我们的责任：

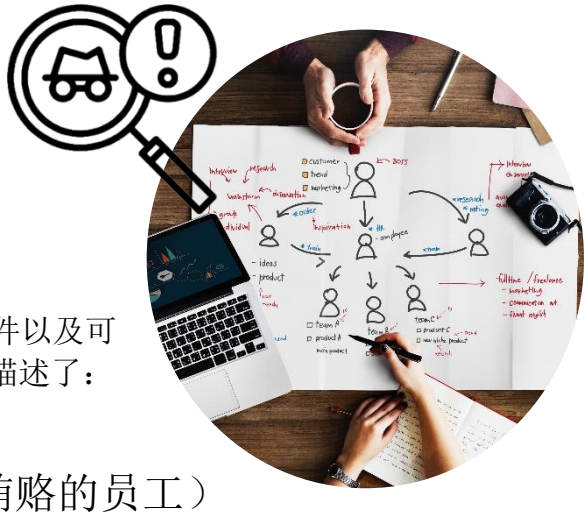
我们：

- 必须遵守有关个人数据保护的地方法规和集团政策规定。
- 必须将任何新的数据处理或更改情况告知数据保护官。
- 除非出于特定合法的必要目的，否则不得收集、使用、披露或存储具有个人性质的数据。
- 必须确保已通知个人其数据正在被收集。
- 必须在数据收集、处理、使用、传播、存储或传输期间保护这些数据。
- 必须确保已处理数据的安全性和机密性。
- 必须仅在处理所需的时间内保留数据，并遵守适用法律。
- 必须在发生涉及个人数据的安全事件时与数据保护官联系。

我们培训员工，改进内部流程。

主页

隐私风险



什么是隐私风险？

风险是一种假设场景，描述了一个令人担忧的事件以及可能导致此事件发生的所有威胁。更具体地说，它描述了：

- 风险源是如何（例如：被竞争对手贿赂的员工）
- 利用配套资源的漏洞（例如：允许处理数据的文件管理系统）
- 在具有威胁的情况下（例如：通过发送电子邮件滥用数据）
- 以及如何使令人担忧的事件发生（例如：非法访问个人数据）
- 涉及个人数据（例如：客户文件）
- 从而对数据主体的隐私产生影响（例如：垃圾邮件、隐私受到侵犯的感觉、个人问题或职业问题）。

不确定性对隐私的影响

严重性代表风险的程度。风险评估主要基于对数据主体的潜在影响程度（**客观**、**实质**、**道德**方面），并考虑现有的、计划的或其他的控制措施。

示例：

职业警报系统使举报人所面临的最重要风险是：由于揭露事实而对其采取报复、歧视或纪律处分的风险。

我们认为：

个人权利的运用与数据处理过程中的风险等级完全无关。

但是，我们有必要根据个人数据处理操作对个人基本权利和自由构成的风险等级来调整数据保护合规性。

《通用数据保护条例》推进了这种做法。因此，对个人基本权利和自由带来较低风险的数据处理操作通常产生较少的合规义务，而“高风险”处理操作将增加额外的合规义务，如数据保护影响评估（DPIA）[1]

我们的责任：

风险评估至关重要。根据《通用数据保护条例》，组织问责制和所有数据处理都要考虑风险因素。

高风险处理所需的数据保护影响评估必须包含风险评估，并与《通用数据保护条例》其他许多要求挂钩，包括数据安全、安全性和数据泄漏通知、隐私设计、合法权益、用途限制及公平处理。

（1）：请参阅第 58 页的定义。

发生违规时的风险

未遵守数据保护法律法规（如《通用数据保护条例》）的法人和自然人面临以下形式的制裁风险和经济损失风险：

刑事制裁：

- 监禁。
- 针对法人实体的罚款。

民事制裁：

- 民事损害赔偿。

行政制裁：

- 正式通知。
- 警告。
- 强制令。
- 暂时或最终的数据处理限制。
- 对某项认证的撤销或撤销某项认证的强制令。
- 暂停数据传输。
- 停止数据处理或撤消授权的强制令。
- 公布已实行的制裁。
- 未经事先正式通知的制裁（紧急情况下）。
- 行政罚款，视违规而定。

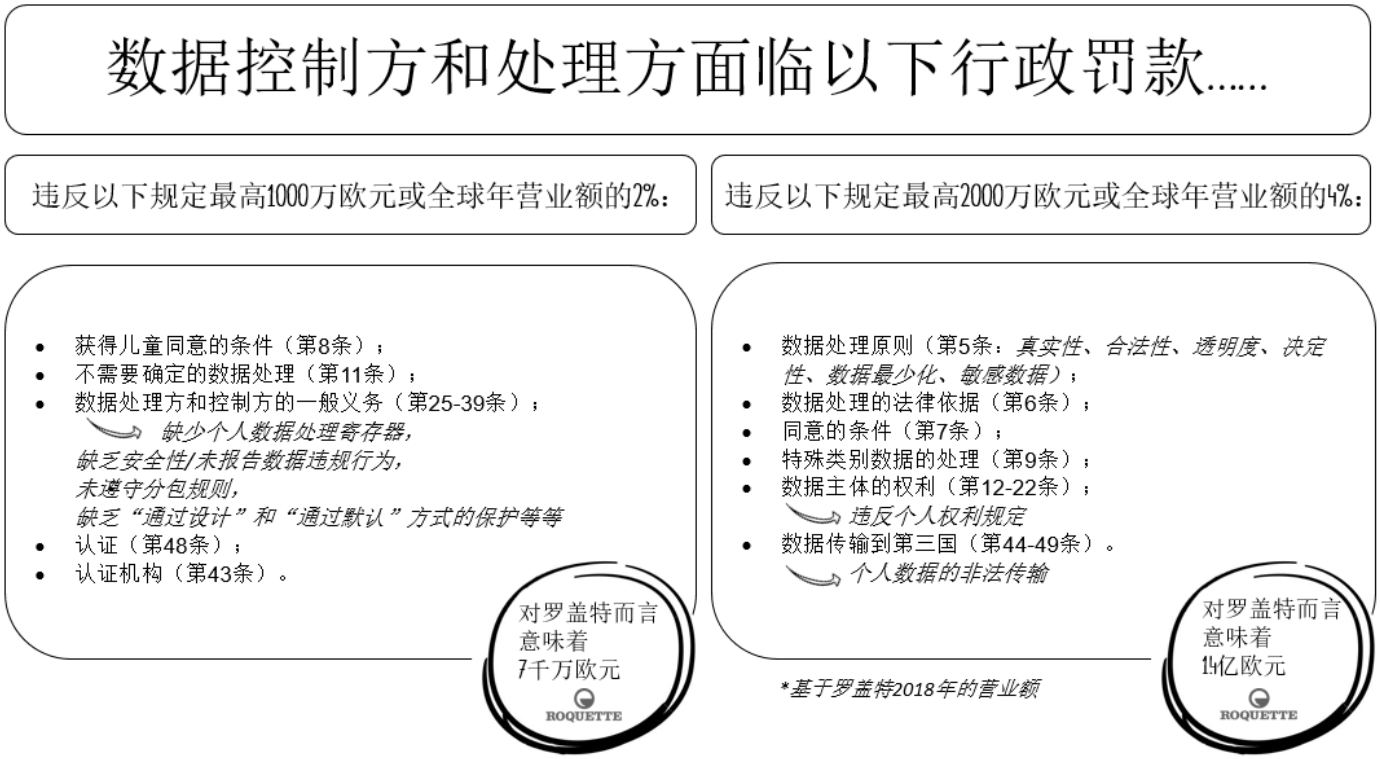
重大经济损失：

- 由于声誉受损而造成的收入损失。

《通用数据保护条例》规定的最高行政罚款是多少？

罚款酌情行事，并非强制。必须根据具体情况实行罚款，并且应“卓有成效、金额合理、具有劝诫作用”。

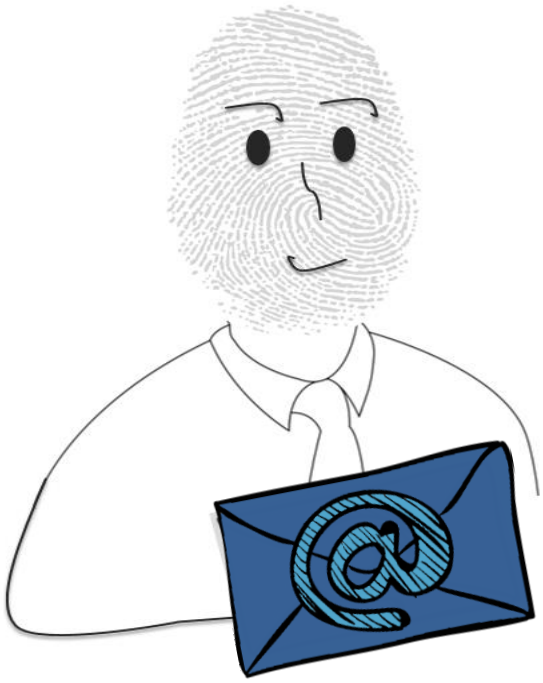
具体罚款金额以组织违反该《条例》特定条款为基础。



什么是刑事制裁？

比如法国法律规定：

- 以欺诈、不正当或非法手段收集个人数据的行为，应处以五年监禁及 30 万欧元罚款（刑法第 226-18 条）。
- 为了保障举报人真正享有权利并受到保护，反腐败法（Sapin II）对阻碍举报的行为严加惩罚。对举报的方方面面进行保密是监管的基本要素。因此，除司法机关外，泄漏举报的机密内容（举报人身份、被举报人身份、为举报提供的证明信息）应处以两年监禁及 3 万欧元的罚款 。



1 我们与数据主体关系的标准

隐私文化

数据保护是一套指导个人数据收集和使用的法律、法规和最佳做法。

个人数据指与某一确定的个人或可识别的自然人相关的任何信息。

数据隐私指处理个人数据。

涉及谁？

在我们的组织中，数据隐私关乎人人，人人有责。

数据隐私为什么很重要？

数据误操作可能对组织、员工及客户造成严重影响。

隐私泄漏可能会造成无限度的财务罚款、负面报道、声誉受损、客户信任损失、业务损失、员工流失、投诉等，如果是自身的个人数据发生隐私泄漏情况，还可能招致诉状，其它情况下也可能招致纪律处分。恰当处理数据关乎我们所有人的利益。

我们认为：

- 罗盖特所有员工都必须了解其在保护个人数据方面的角色和责任。提高认识旨在加强罗盖特内部对尊重隐私和保护个人数据的企业文化。

[DDPG001EN – 规则 1]

- 必须对员工开展个人数据保护政策实施培训。

[DDPG001EN – 规则 2]

考虑隐私

这是我们的责任！

为实现业务成功，我们需要客户和员工的个人资料。

保护这些重要的信息，我们是值得信赖的。

每名员工都有责任遵守相应的数据保护法。

这是我们的声誉！

获得声誉很难，但失去声誉却很容易。

小心谨慎地处理客户和员工资料对于保护我们的声誉是至关重要的。

您是防止声誉受到损害的最佳捍卫者。

这关系到尊重！

要想保持客户和员工对我们的信任，必须尊重他们做出的关于怎样使用其个人数据的选择。

这掌握在您的手中！

我们都要负责保证客户和员工的个人数据安全、保密。

对于需要发送或带走的信息，必须要格外小心。

了解更多……

- 《行为守则》 – 隐私和数据保护 – 第 42-43 页。
- 对于新员工：全球入职培训期间提供有关数据保护的部分信息和在线学习。
- 对于现有员工：学习内容上传至“Workday 学习”平台。
- 对于数据保护协调员：相关文档共享在我们的社群“数据保护网络”中。
- 面向所有人： 更多信息请访问内部门户网站> 数据保护。

个人数据 处理

个人数据处理是指任何一个或一套关于个人数据或个人数据集的操作，不论其是否通过自动化手段执行，如收集、记录、组织、构建、存储、改编或变更、检索、咨询、使用、通过传输传播披露或以其他方式提供、排列或组合、限制、消除或破坏。

您需要注意的一项数据保护（及《通用数据保护条例》）要求是，您需要有“合法依据”才能收集个人数据。

合法依据可能会根据当地法规而有所不同。

我处理个人数据的“合法依据”是什么？

您要能清楚地回答这个问题：

“你是如何得到我的[数据]，以及为什么你被允许得到它？”

更具体一点就是，这意味着您需要符合处理数据的六项合法依据中的至少一项。根据《通用数据保护条例》，除非满足以下条件，否则您不能处理任何数据：

1. 同意
2. 合同
3. 法律义务
4. 重要利益
5. 公共任务
6. 合法利益

合法、公正、透明

我们的责任：

我们必须运用各项规则，确保个人数据的合法处理。

规则	Q-Docs 标准	《通用数据保护条例》标准
• 收集数据时做到合法、公正、透明	DDPG002EN 规则 1	第 5 1. a）条
• 证明已获得有关人员的同意（必要时）	DDPG002EN 规则 2	第 7 条
• 遵守数据收集过程中确定的用途	DDPG002EN 规则 3	第 5 1. b）条
• 在严格必要限制范围内以纸质或数字形式收集信息	DDPG002EN 规则 4	第 5 1. c）条
• 将数据保留限制在严格必要的范围内	DDPG002EN 规则 5	第 5 1. e）条
• 采取措施将个人数据传输到第三国或国际组织	DDPG002EN 规则 6	第 44-50 条

我们培训员工，改进内部流程。

数据主体的权利

数据主体是指可以被直接或间接识别的自然人，特别是通过参考标识符，如姓名、身份证号、位置数据、在线标识符、或该自然人在身体、生理、遗传、心理、经济、文化或社会身份方面的一个或多个特定因素。

什么是“数据主体”？

这是特定个人数据所涉及的个人的技术术语。

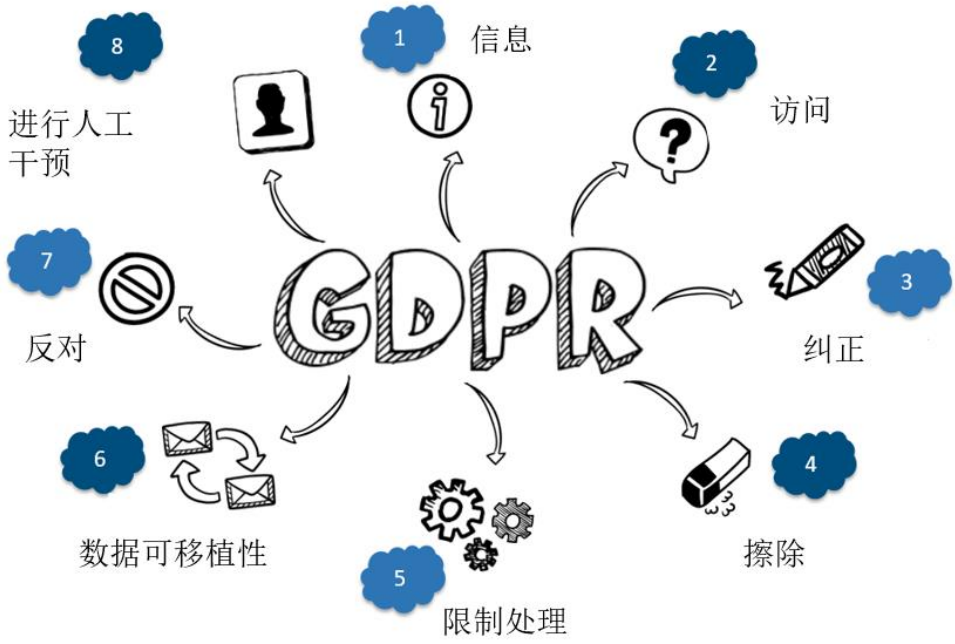
什么是主体访问请求？

现行数据保护法赋予个人的主要权利之一就是对其个人信息的访问权。

个人可以向您发送“主体访问请求”，要求您告诉他/她您所拥有的关于他/她的个人信息，并向其提供该信息的副本。在大多数情况下，您必须在收到有效主体访问请求后 30（*）个日历日内做出回应。

（*）：这个期限可能会根据适用法律或数据处理操作的性质而有所不同。

什么是其他数据主体的权利？



我们的责任：

我们必须运用各项规则，确保数据主体的权利。

规则	Q-Docs 标准	《通用数据保护条例》标准
• 确保法律通知符合义务	DDPG006EN 规则 1	第 12 条
• 允许数据主体行使其访问权	DDPG006EN 规则 2	第 15 条
• 允许数据主体行使其纠正权	DDPG006EN 规则 3	第 16 条
• 允许数据主体行使其数据可移植性权	DDPG006EN 规则 4	第 20 条
• 允许数据主体行使其擦除权（“被遗忘权”）	DDPG006EN 规则 5	第 17 条
• 允许数据主体行使其数据处理限制权	DDPG006EN 规则 6	第 18 条
• 通知个人数据的纠正或擦除情况或数据处理的限制情况	DDPG006EN 规则 7	第 19 条
• 控制自动化个人决策，包括数据剖析	DDPG006EN 规则 8	第 22 条

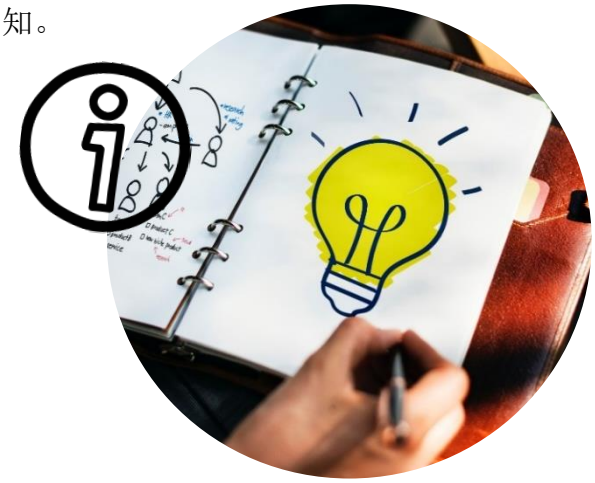
我们培训员工，改进内部流程。

隐私声明

个人数据正在被使用的告知权

作为罗盖特员工的您以及与罗盖特有关系的所有第三方，如果我们正在使用您/他们的个人数据，我们必须要予以告知。

我们应提供以下详细信息：



- 罗盖特使用您/他们的数据的原因。
- 罗盖特正在使用的一个或多个数据种类。
- 您/他们的数据的保留期限。
- 您/他们的信息权。
- 这些数据的来源。
- 罗盖特是否要将您/他们的数据传输给第三方的相关信息，包括您/他们的姓名及传输原因。
- 有关是否打算在其他管辖区传输数据的信息，包括相关国家以及如何处理这些数据。
- 罗盖特是否将这些数据用于数据剖析（一种自动化处理，其中其个人数据用于分析或预测您的工作绩效、经济状况、健康状况等信息）。
- 数据保护官的联系方式。
- 有疑问时您/他们向监管机构投诉的权利。

这被称为**隐私信息**或**隐私声明**。

在罗盖特收集您的数据时，我们应向您/他们提供隐私信息。如果罗盖特从其他来源获得您/他们的数据，则应提供隐私信息。这可以以隐私声明的形式进行。

这被称为**知情权**。

规则	Q-Docs 标准	《通用数据保护条例》标准
• 确保法律通知符合义务	DDPG006EN 规则 1	第 12 条

示例：

- 罗盖特网站隐私信息请访问：https://www.Roquette.com/data-protection。
- 有关 Workday@Roquette 人力资源流程的隐私信息请访问 ONE 平台：员工天地 > Workday@Roquette。

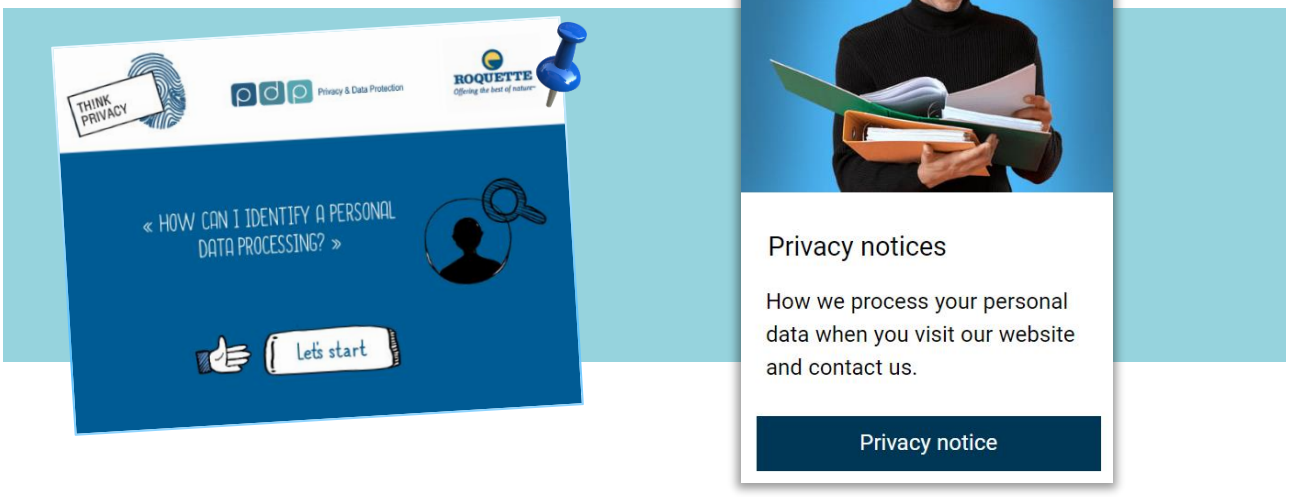
罗盖特何时可以不将其活动告知您/他们？

通常，我们必须向您/他们提供隐私信息，但在某些情况下我们不必这么做。这些情况包括：

- 您/他们已得到隐私信息，并且没有发生任何更改，
- 无法向您提供隐私信息或者需要“不合情理的努力”，或
- 向您提供隐私信息后会造成无法使用您的数据或对使用这些数据的原因造成严重影响。

注：如果需要采取临时措施以避免证据被隐藏或受到破坏，则可以在采取临时措施后再发布此类信息。

我们培训员工，改进内部流程。



数据最小化

什么是数据最小化原则？

《通用数据保护条例》第 5（1）（c）条规定：

> “1.个人数据应：
>
> （c）充分、相关且限于与处理目的有关的必要内容（数据最小化）”

各个全球职能部门设计的用于收集个人数据的纸质或数字化形式应仅包含出于处理目的严格必需的信息字段，避免收集没有正当处理理由的数据。

我们的责任：

我们必须确保您正在处理的个人数据：

- 充分：足以恰当实现您的既定目的；
- 相关：与该目的存在合理联系；及
- 仅限于必要的内容：您所拥有的数据不超过此目的所需的范围。

规则	Q-Docs 标准	《通用数据保护条例》标准
• 在严格必要限制范围内以纸质或数字形式收集信息。	DDPG002EN 规则 4	第 5 1. c）条

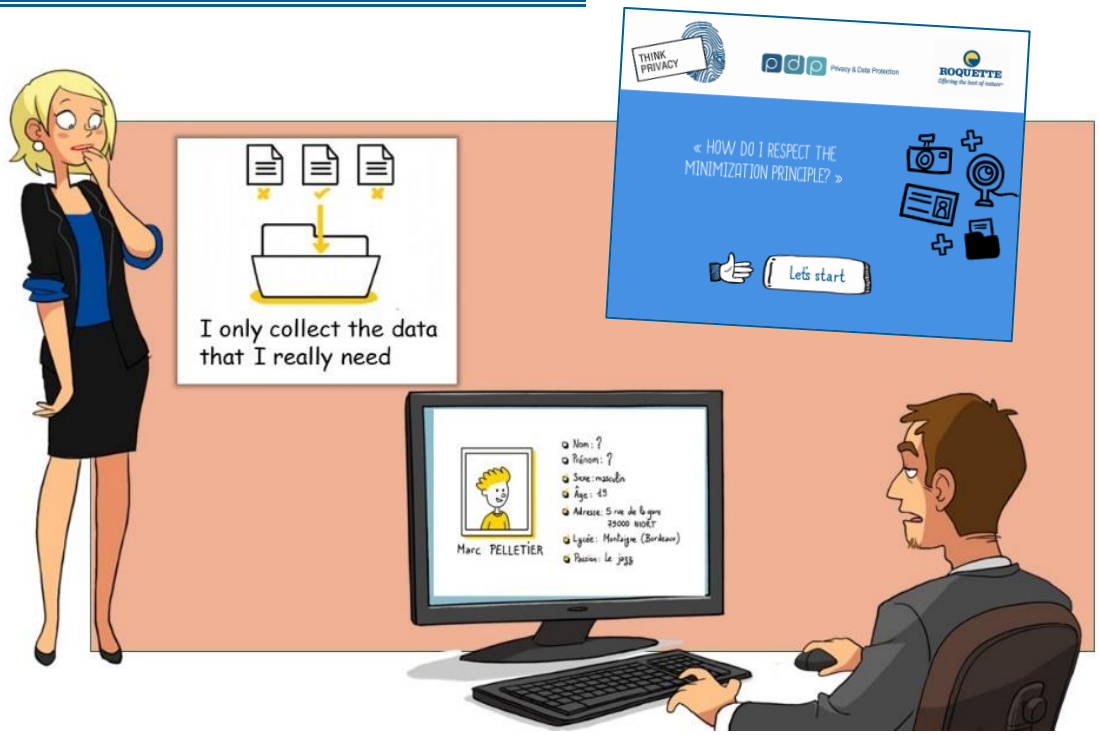
检查表：

- ☑ 我们仅收集特定目的所需的个人数据。
- ☑ 我们拥有的个人数据足以恰当实现这些目的。
- ☑ 我们会定期审查持有的数据，并删除不需要的一切内容。
- ☑ 我们应确定实现您的目的所需的最少个人数据量。我们应持有那么多的信息量，但不会超过这个量。

问责制原则意味着您需要证明自己具有适当的流程，以确保仅收集和保存所需的个人数据。

还请记住，《通用数据保护条例》规定，根据纠正权条款，在数据不足以实现您的目的时，个人有权补充完整这些不完整的数据。根据擦除权（被遗忘权）条款，他们还有权让您删除任何不必要的数据。

我们培训员工，改进内部流程。



数据安全

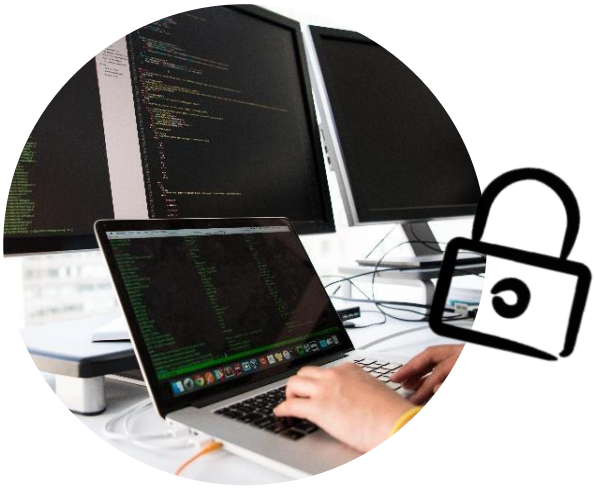
网络安全是一种横向活动，实施网络安全可确保相关信息和资产在适当且有保证的保护级别下共享和使用数据：

- **机密性**：确保信息保密，不会泄露给不适当的个人或实体；
- **完备性**：维护信息和处理方法的准确性和完整性；
- **可用性**：确保授权用户在需要时始终可以访问信息应用程序及服务；
- **可追溯性**：指保留相关记录以及在需要时保留我们系统相关操作证据的能力。可追溯性还涵盖法律目的，例如不可否认性或问责制。

个人信息资产包括：

- 纸质文件（文本、地图、图片等）；
- 办公环境中的数字化信息；
- 移动环境中的数字化信息；
- 专业知识和技能（个人拥有或口头分享的）；
- 实物（如样品、菌株、模型等）。

[DSUG006EN]网络安全管理指令



假名是指按照以下方式处理个人数据：在不使用附加信息的情况下，无法再将个人数据归因于特定数据主体，但前提是此类附加信息应单独保存并受技术措施和组织措施的约束，以确保个人数据不会归因于已识别或可识别的自然人。

匿名是指这样的一个过程：通过该过程不可逆地更改个人数据，从而再也无法单独通过数据**控制方**[1]或与其他第三方协作而直接或间接地识别数据主体。

加密是指这样的一种方法：通过该方法，纯文本或其他任何类型的数据从可读形式转换为编码数据，而其他实体只有在可以访问解密密钥的情况下，才能解码这些编码数据。加密是保证数据安全的最重要方法之一，尤其适合跨网络传输数据的端到端保护。

（1）：请参阅第 38 页的定义。

我们认为：

为了维护数据安全并防止处理数据时违反数据保护法律法规，罗盖特及我们的分包商应评估数据处理中固有的风险，并采取**加密**或**假名**等措施来减轻这些风险。

我们的责任：

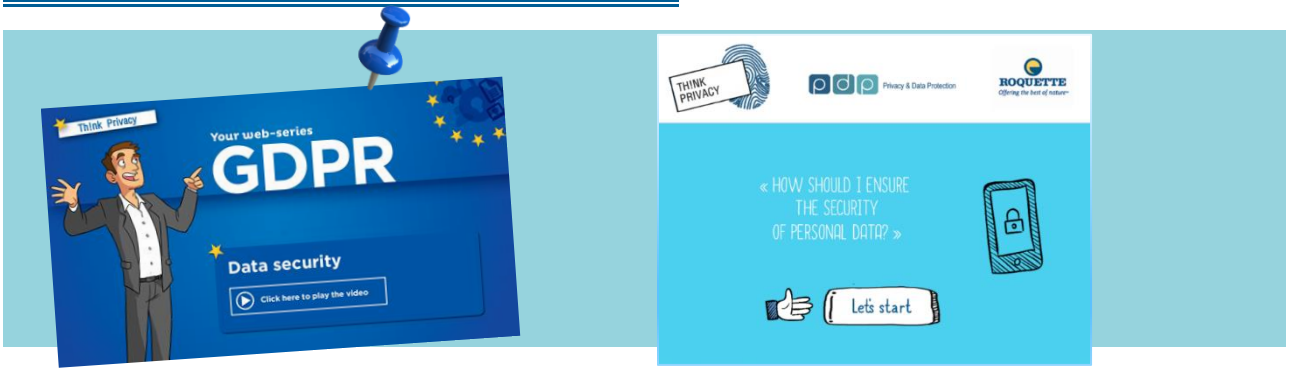
在我们处理任何类型的个人数据时，都需要采取安全措施，但具体要采取什么措施则取决于特定情况。我们需要确保用于处理个人数据的系统和服务的机密性、完备性及可用性。

这可能包括信息安全策略、访问控制、安全监控及数据恢复计划等等。

在个人数据整个生命周期间，所有利益相关方都必须采取适当的安全措施。

规则	Q-Docs 标准	《通用数据保护条例》标准
• 运用并审查安全策略和指令中规定的安全措施	DDPG007EN 规则 1	第 32 条
• 将信息安全和数据保护审查纳入到项目中。	DDPG007EN 规则 2	第 32 条
• 通过设计和默认方式实现安全、隐私及数据保护	DDPG007EN 规则 3	第 25 条
• 将信息安全和数据保护条款纳入到分包商合同中	DDPG007EN 规则 4	第 32 条

我们培训员工，改进内部流程。



个人信息分类

除特殊情况外，禁止处理敏感个人数据及某些特殊类别的个人数据。

处理这些数据时需要采取以下保护措施：

标记、访问、传输、运输、复印和打印、存储和归档、销毁。

分类旨在识别敏感信息资产（无论其性质和载体如何），并在必要时指定保护措施，以减少意外泄漏后产生的风险。

机密性分类级别与信息意外泄露产生的评估影响直接相关。

[DSUG001EN]信息保护指令

信息保护分级	个人数据类型	个人数据类别
级别1-罗盖特限制信息 定义：不建议公开广泛披露的信息类型	普通个人数据	公民状况、身份、身份数据
		个人生活（生活习惯、婚姻状况，敏感数据除外）
		职业生涯（简历、学历和专业培训、获奖情况）
		经济信息和财务信息（收入、财务状况、税收状况）
		连接数据（IP地址、事件日志）
		位置数据（出行、GPS数据、GSM数据）
级别2-罗盖特机密信息 定义：披露后可能会对集团利益重大损害的信息类型	被认为敏感的个人数据	社会保障号码
		生物识别信息
		银行数据
级别3-罗盖特绝密信息 定义：披露后可能会对集团利益造成严重损害的信息类型	敏感个人数据 在《数据保护法》规定的含义下	哲学观点、政治观点、宗教观点及工会观点、性生活、健康数据、种族或族裔
		犯罪、定罪、安全措施

我们的责任：

规则	Q-Docs 标准	《通用数据保护条例》标准
• 遵守敏感数据处理的法律框架	DDPG004EN 规则 1	第 9 条
• 禁止处理有关刑事定罪和犯罪的数据	DDPG004EN 规则 2	第 10 条
• 仅限授权专业人员访问健康数据	DDPG004EN 规则 3	第 9 条
• 禁止将身份证号码作为唯一识别码使用	DDPG004EN 规则 4	第 87 条
• 限制访问和使用银行数据	DDPG004EN 规则 5	第 9 条
• 仅限授权人员访问敏感数据	DDPG004EN 规则 6	第 9 条
• 对敏感数据处理中涉及的数据主体的隐私进行影响评估	DDPG004EN 规则 7	第 35 条
• 将注释字段的使用范围限制为一般信息	DDPG004EN 规则 8	最佳做法

部分实用技巧……

对各类机密信息资产（纸质信息、数字化信息、专有技术、实物）应采取的保护措施示例。

数据保留

罗盖特集团及其客户和业务合作伙伴之间日益增长的对于非物质化操作和信息交流的需求以及法律法规要求，使罗盖特在数据保留期限和记录管理政策方面受到大量义务的约束。

在业务开展过程中，罗盖特会获取并处理与我们的战略、财务业绩、商业发展或承诺相关的大量敏感数据，**以及与我们的客户、业务合作伙伴及员工相关的个人数据**。

罗盖特发送或接收的与业务有关的信息，**除非包含个人信息**，否则即使没有任何阻止公司将其长时间保留在档案中的情况，保留的期限也只限于最短保留期限。

行政机关和主管当局可以在此期限内进行事后检查，而该期限根据要保留的信息性质及相关的法律要求而有所不同。

禁止无限或不确定的存储时间。

《通用数据保护条例》第5 1.E）条

“存储限制”

个人数据的保存方式应使数据主体识别出的时间不超过处理个人数据目的所需的时间。

个人数据可能会保存更长的时间，但仅限于出于公共利益、科学研究、历史研究或统计的目的而对个人数据进行存档处理，同时必须采取恰当的技术措施和组织措施，从而维护数据主体的权利和自由。

我们的责任：

- 作为数据控制方，我们必须为收集和处理的每类个人数据规定具体而充足的存储时间。
- 在处理个人数据之前，项目负责人必须在数据保护协调员的协助下在我们的注册簿中指定数据保留的期限。
- 我们必须仅在处理所需的时间内保留个人数据，并遵守适用法律。

规则	Q-Docs 标准	《通用数据保护条例》标准
• 将数据保留限制在严格必要的范围内	DDPG002EN 规则 5	第 5 1.E）条

在这方面，各个全球职能部门、全球事业部及区域致力于遵守公司信息保留规则，并坚持实施相关程序。

示例：

在招聘流程结束时，对于未录用的应聘人员，除非他们同意在限定时间（2 年）内留在我们的“人才库”中，否则我们必须删除他们的相关信息。

我们培训员工，改进内部流程。

2 我们与数据主体和分包商关系的标准

数据处理方和控制方的资格

控制方是指单独或与他人共同确定处理个人数据的目的和方式的自然人或法人、公共机关、机构或其他组织。

共同控制方是指共同决定数据处理的目的和方式的两个或两个以上的控制方。但是，无论如何安排，每个控制方都仍旧有责任遵守《通用数据保护条例》规定的控制方的所有义务。

处理方是指代表控制方处理个人数据的自然人或法人、公共机关、机构或其他组织。

《通用数据保护条例》中所指的处理方是谁？

（《通用数据保护条例》第4条：定义）。
从该术语的法律意义上讲，**各种各样的服务提供商都能成为处理方**。处理方的活动可以涉及非常具体的任务（邮件投递的分包），也可以涉及更加普遍、范围更广的内容（代表另一个组织管理整项服务，如管理员工的工资）。

《通用数据保护条例》特别关注以下内容：

- 有权访问数据的 IT 服务提供商（托管、维护等）、软件集成商、网络安全公司或 IT 咨询公司（以前称为 IT 工程服务公司），
- 代表客户处理个人数据的营销机构或传播机构，及
- 更笼统地说，代表另一个组织提供个人数据处理服务的任一组织，
- 公共机构或协会也可以被视为是此类组织。

软件发行商和设备制造商（例如时钟终端、生物识别设备或医疗设备）如果无法访问或处理个人数据，则不在此列。

数据处理方和控制方的资格要求示例：

A 公司使用 B 公司和 C 公司的客户数据文件提供营销信函投递服务。

只要 A 公司是代表 B 公司和 C 公司并根据 B 公司和 C 公司的指示而处理发送信函所需的客户数据，则 A 公司是 B 公司和 C 公司的数据处理方。

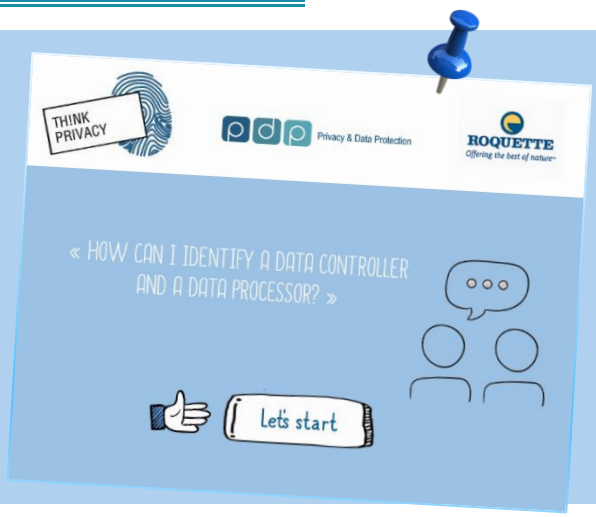
B 公司和 C 公司是他们客户的管理控制方，包括在营销信函的投递方面。

A 公司还是其雇用的员工以及包括 B 公司和 C 公司在内的客户的管理控制方。

官方案文

- 《通用数据保护条例》第 4 条关于控制方和处理方的定义
- 《通用数据保护条例》第 28.10 条有关控制方的概念

我们培训员工，改进内部流程。



数据保护条款

什么时候需要合同以及合同为什么很重要？

作为数据控制方，我们每次聘用数据处理方来代表我们处理个人数据时，双方都需要订立书面合同。
合同很重要，可以使双方了解彼此的职责和责任。

作为数据控制方的罗盖特与其数据处理方之间签订的包含具体数据保护条款的合同和/或数据保护协议，确保双方了解彼此的义务、职责及责任。合同还有助于我们遵守《通用数据保护条例》，并有助于我们在问责原则要求时向个人和监管机构证明我们的合规情况。

聘用数据处理方时，我们作为数据控制方有哪些职责和责任？

我们只可聘用能够提供足够保证的数据处理方，保证他们将采取恰当的技术措施和组织措施，以确保其数据处理符合《通用数据保护条例》要求并保护数据主体的权利。

作为数据控制方，我们主要负责全面遵守《通用数据保护条例》及其他现行的数据隐私法，并负责证明做到合法合规。如果未实现这一点，则我们可能要负责支付法律诉讼赔偿金，或受到罚款或其他处罚措施或纠正措施的处罚。

《通用数据保护条例》的新规定有哪些？

《通用数据保护条例》把数据控制方与处理方之间的书面合同作为一项要求，而不仅仅是证明其已遵守现行数据保护法规定的数据保护原则（恰当的安全措施）的一种方式。

现在，这些合同必须包含特定的最低条款。这些条款旨在确保数据处理方开展的数据处理符合《通用数据保护条例》的所有要求，而不仅仅是与确保个人数据安全相关的要求。

规则	Q-Docs 标准	《通用数据保护条例》标准
• 将信息安全和数据保护条款纳入到分包商合同中。	DDPG007EN 规则 4	第 32 条
• 承包商安全	DSUG016EN	

合同中应包含哪些内容？

合同必须规定：

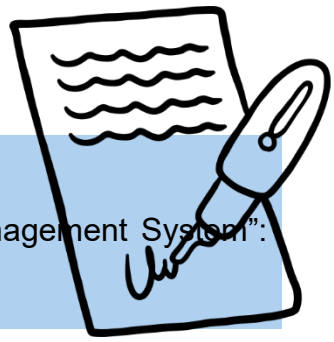
- ☑ 数据处理的主题和期限；
- ☑ 数据处理的性质和目的；
- ☑ 个人数据的类型及数据主体的类别；及
- ☑ 数据控制方的义务和权利。

合同还必须包括有关以下方面的特定条款：

- ☑ 仅按照数据控制方的书面说明进行处理；
- ☑ 保密义务；
- ☑ 相应的安全措施；
- ☑ 使用子处理器；
- ☑ 数据主体的权利；
- ☑ 配合数据控制方；
- ☑ 合同终止条款；及
- ☑ 审计与检查。

我们培训员工，改进内部流程。

- 符合《通用数据保护条例》的分包合同数据保护指南。
- « Data Processing Agreement” 模板可在我们的 “Privacy Management System”: OneTrust@Roquette> “Vendor Risk Management” 模块。



数据传输协议

数据传输是指将个人数据进行传播、复制或搬移（如托管服务器、通过电子邮件发送附件、远程访问工具、屏幕共享等），目的是在有着不同的适用个人数据保护法的其他国家进行处理。

这是一个空前互联互通的时代。罗盖特在全球范围内开展业务，因此数据的国际传输是日常业务运营的重要组成部分。例如，罗盖特将员工的个人数据存储在国外托管的云服务平台上，并在全球各地的子公司之间共享员工和客户的个人数据。

《通用数据保护条例》及其他现行数据保护法将如何影响此类国际数据传输？

我们的责任：

仅在以下情况下，才能传输正在处理或打算在传输到第三国或国际组织之后进行处理的个人数据：

- 当地法律允许传输，和/或监管机构决定，第三国、该第三国境内的某个领土或一个或多个指定部门、或有关国际组织，确保提供充分的保护或授权; 和/或
- 已采取法律措施（如：根据欧洲议会和欧洲理事会 95/46/EC 指令等规定，针对将个人数据传输到在第三国境内设立的数据处理方的企业约束规则或标准合同条款）。

规则	Q-Docs 标准	《通用数据保护条例》标准
• 采取措施将个人数据传输到第三国或国际组织	DDPG002EN 规则 6	第 44-50 条

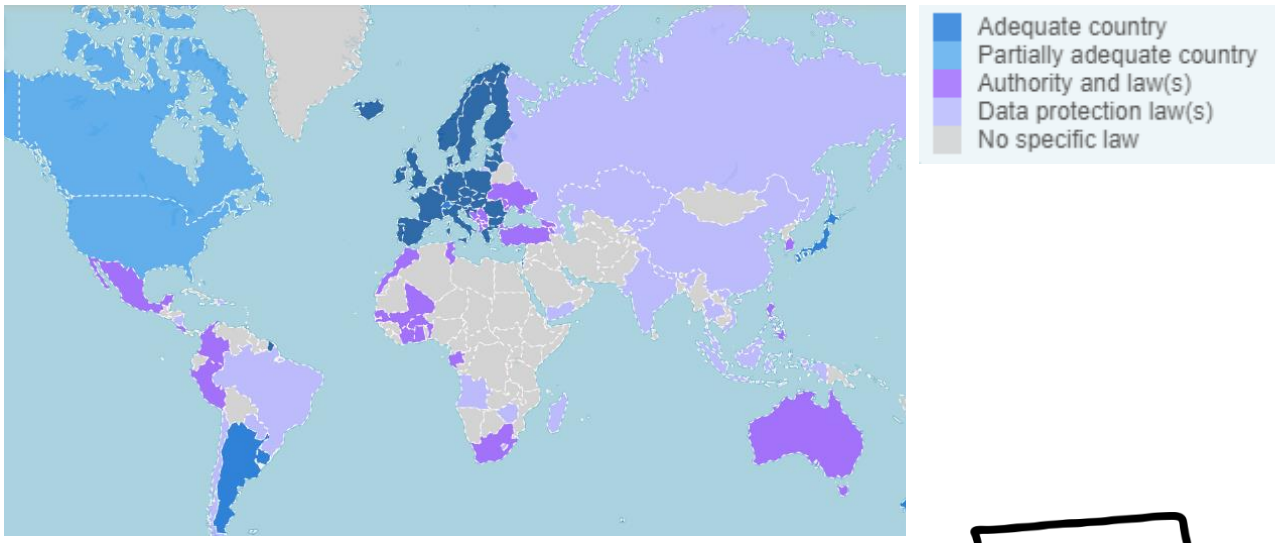
无论出现何种情况，请先联系数据保护官。

我可以在哪个国家以及在何种情形下传输个人数据？

请查阅该地图了解概况：

https://www.cnil.fr/en/data-protection-around-the-world。

该地图使您可以查看每个国家的数据保护级别。



了解更多……

- “Data Transfer Agreement” 部分，包括在我们的 “Data Processing Agreement” 模板。
- 常见问题解答，旨在回答“欧盟委员会关于将个人数据传输到在第三国设立的数据处理方的标准合同条款的决定”实施生效所引起的一些问题。

3 我们与网络和监管机构关系的标准

数据保护官

集团已任命了一名数据保护官。

数据保护官（DPO）协助我们监督内部合规情况，提供数据保护义务方面的信息和建议，提供数据保护影响评估（DPIA）方面的建议，并对接数据主体和监管机构。

数据保护官必须是数据保护领域的专家，具有独立性，拥有充足的资源并向最高管理层报告。

数据保护官可以帮助我们证明合规情况，并在更加注重问责制方面起作用。

数据保护官的任务	Q-Docs 标准	《通用数据保护条例》标准
• 我们数据保护官的任务是监督在《通用数据保护条例》及其他数据保护法律、集团数据保护政策、宣传教育、培训及审计方面的合规情况。	MDPG001EN 个人数据保护手册	《通用数据保护条例》第 39 条 数据保护官的任务
• 我们将考虑数据保护官的建议及其提供的数据保护义务信息。		
• 在开展数据保护影响评估时，我们会征求数据保护官的意见，并且数据保护官还会监督评估流程。		
• 数据保护官负责对接监管机构。		
• 在执行任务时，数据保护官会充分考虑与数据处理操作相关的风险，并考虑数据处理的性质、范围、背景及目的。		

集团首席执行官已将任命的集团数据保护官上报至法国国家信息与自由委员会，于《通用数据保护条例》生效日期 2018 年 5 月 25 日开始履行职责。

数据保护官的可达性：

- 我们的数据保护官是詹尼弗·戈德温（Jennifer Godin），我们的员工、个人及监管机构可以很方便地联系到她。
- 我们已公开了她的详细联系方式，并将其传达给了监管机构。

  ☑ https://www.Roquette.com/data-protection
  ☑ ONE > 全球职能部门 > 数据保护
  ☑ ONE > 我们的社群 > 数据保护网络

以下情形请联系数据保护官：

☑ 个人数据处理

☑ 数据主体请求

☑ 个人数据泄漏

☑ 需要咨询或协助

统一联系方式：dpo@Roquette.com 或 jennifer.godin@Roquette.com

我们培训员工，改进内部流程。

数据保护网络

各个部门的对接人员及本地数据保护官或协调员组成了一个网络，使集团数据保护官可以分别在每个事业部和支持部门中实施个人数据保护规则，遵守集团运营所在国相关法律法规对数据保护的要求。

本地数据保护官/协调员至少应执行以下任务：

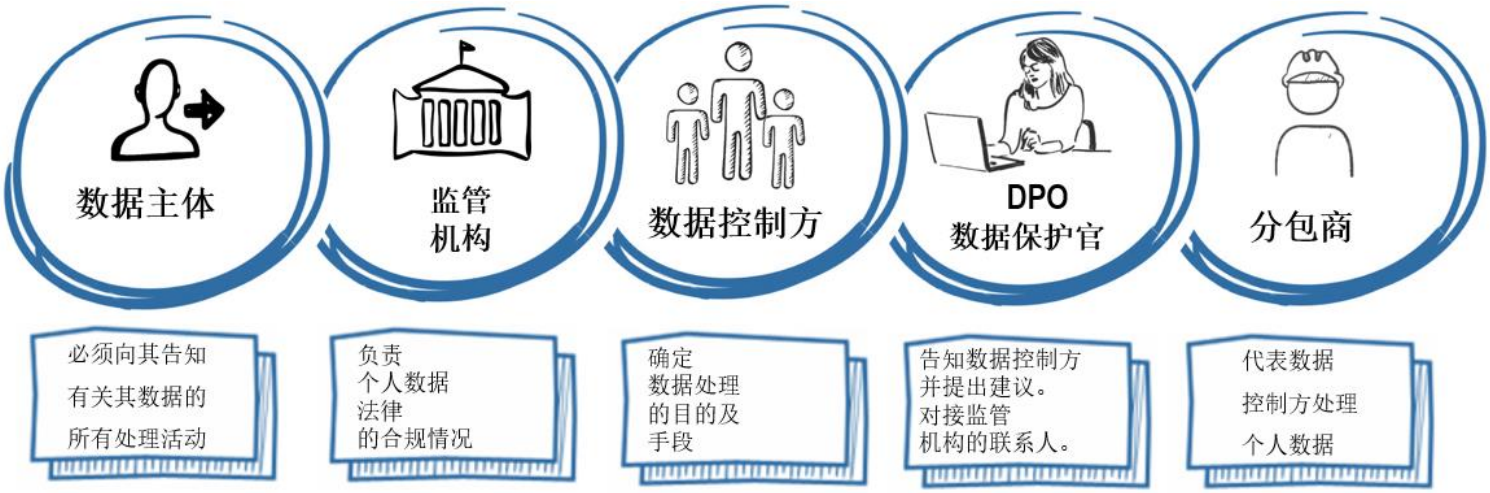
- 在本地层面传达由罗盖特集团数据保护官制定的罗盖特个人数据保护政策义务、以及有关数据保护的当地适用法律要求，并提供建议；
- 必要时，在罗盖特集团数据保护官的协助下，对是否遵守当地法律、涉及数据保护的其他法律和适用法规、以及个人数据保护相关政策的合规情况进行监督；
- 应要求在本地层面提供有关数据保护影响评估的建议，并监督评估情况；
- 配合当地监管机构的工作；
- 在数据处理相关问题方面对接罗盖特集团数据保护官，并在其他事项方面酌情咨询罗盖特集团数据保护官；
- 向罗盖特集团数据保护官报告其工作情况，促进集团数据保护管理系统的建设。

我们培训员工，改进内部流程。

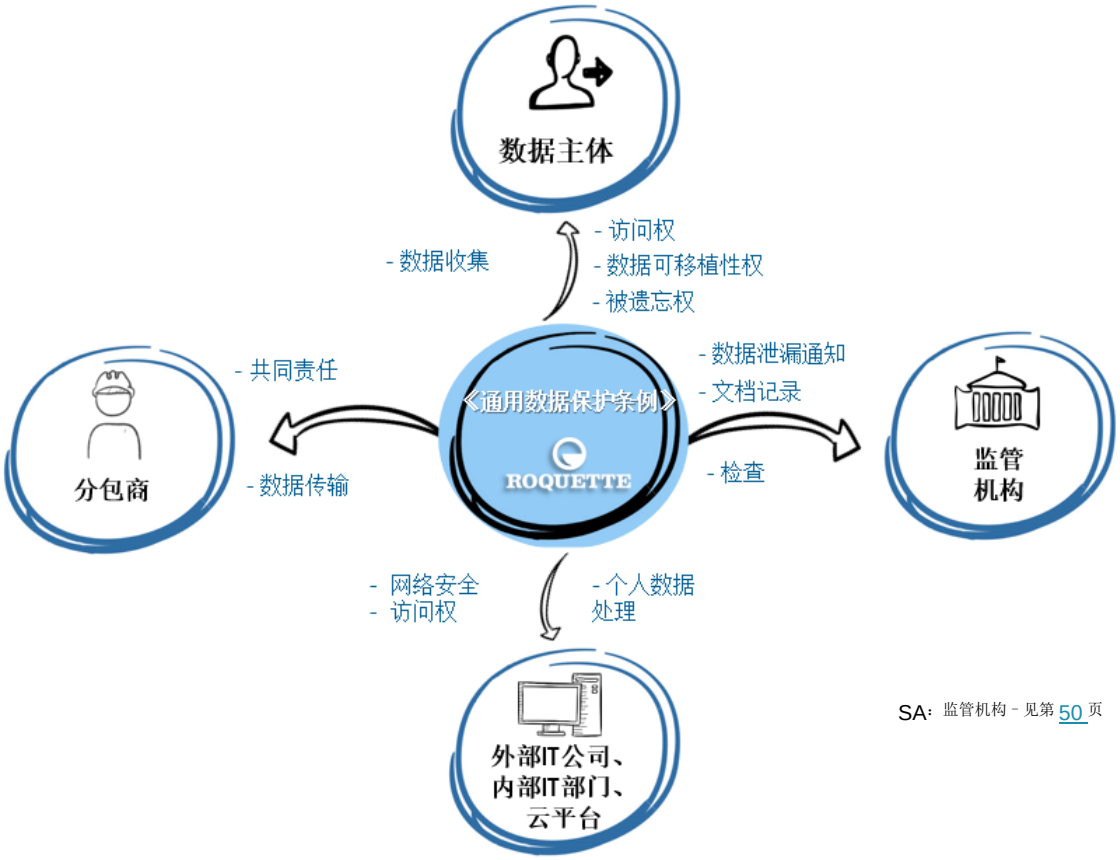
我们的年度 PDP 研讨会是数据保护和隐私贡献者网络的聚会场所。

与利益相关者

谁是新的参与者？



这些利益相关者之间有什么关系？



SA：监管机构 - 见第 50 页

监管机构

全球很多国家都制定了数据保护法并设立了独立的**数据保护机构（DPA）**。

这些机构是针对隐私和信息自由的独立国家监管机构。它们促进并维护数据主体的权利，使数据主体可以访问各个组织拥有的信息，并保护其个人信息。

监管机构在《通用数据保护条例》背景下的作用是什么？

每个成员国应设立一个或多个独立的公共机构，负责监督个人数据和隐私法的实施情况，从而在个人数据处理范围内保护数据主体的基本权利和自由，并促进此类个人数据在欧盟境内的自由流通。

在《通用数据保护条例》的背景下，所有欧盟成员国都应设立数据保护机构，该机构通常充当该成员国内利益相关方的主要对接联络点。

为了确保《通用数据保护条例》在整个欧盟范围内得到统一实施，每个监管机构都必须与其他监管机构及欧洲委员会通力合作。

每个成员国的监管机构都必须使本国公众更加认识和了解与个人数据处理有关的风险、规则、保障及权利。

这些监管机构还负责处理数据保护违规行为，并向各个组织提供咨询和/或协助并回答具体问题。

简而言之，监管机构（SA）的职责包括：

- 确保包括罚款在内的各项规则得到实施；
- 通过指南等手段（如必要）阐明规则的实施方式；
- 推动创建与包括企业在内的所有利益相关方的对话文化；
- 通力合作。

CNIL：法国国家信息与自由委员会 - 法国数据保护机构。

领导机构

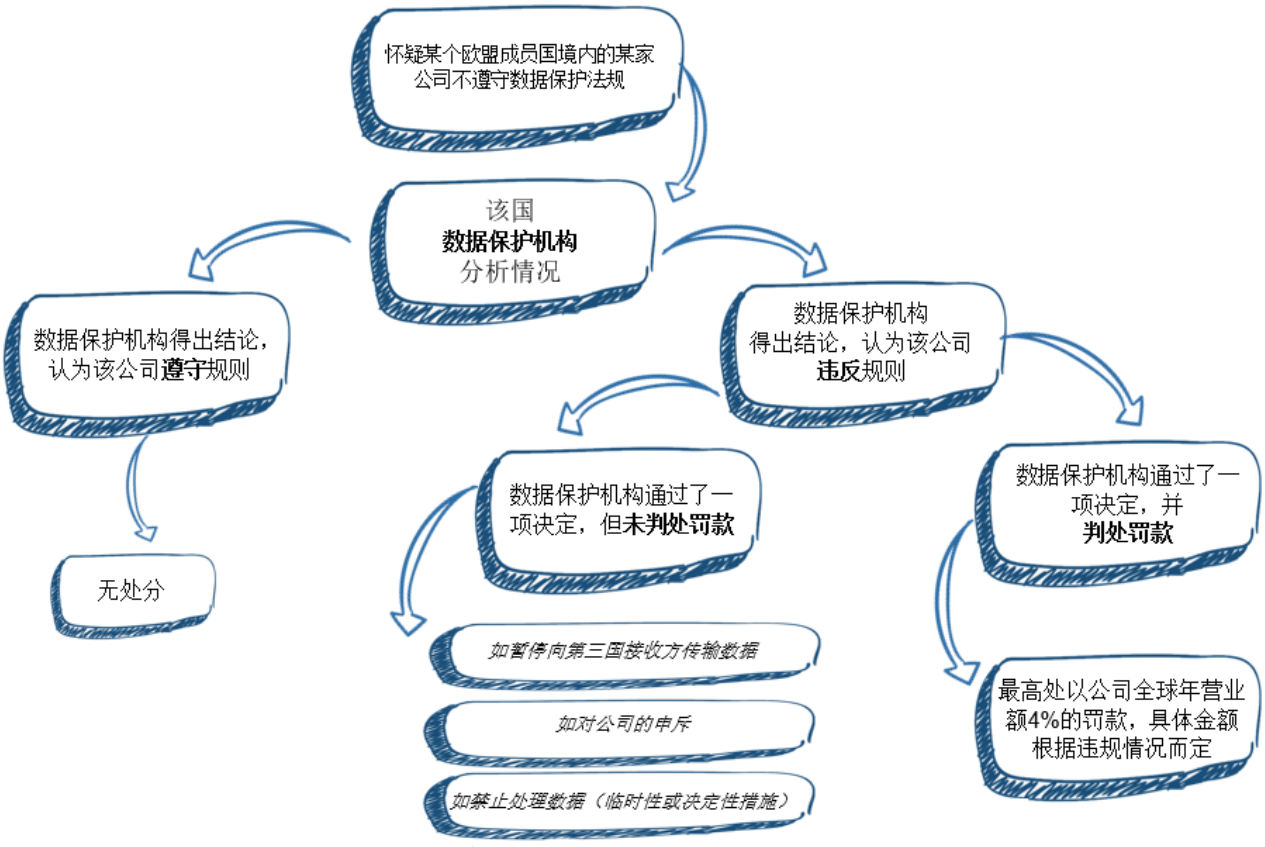
- 数据控制方或处理方总部所在地的监督机构应充当领导机构。领导机构应配合其他相关机构的工作。
- 仅在数据控制方或处理方开展个人数据跨境处理时，才有必要确定领导监管机构。

如何确定“领导监管机构”？

确定主要数据控制方总部在欧盟境内的位置。
该控制方总部所在国的监官机构就是该控制方的领导机构。

法国国家信息与自由委员会*是罗盖特的领导监管机构*

《通用数据保护条例》制裁机制在实践中如何运作？



治理

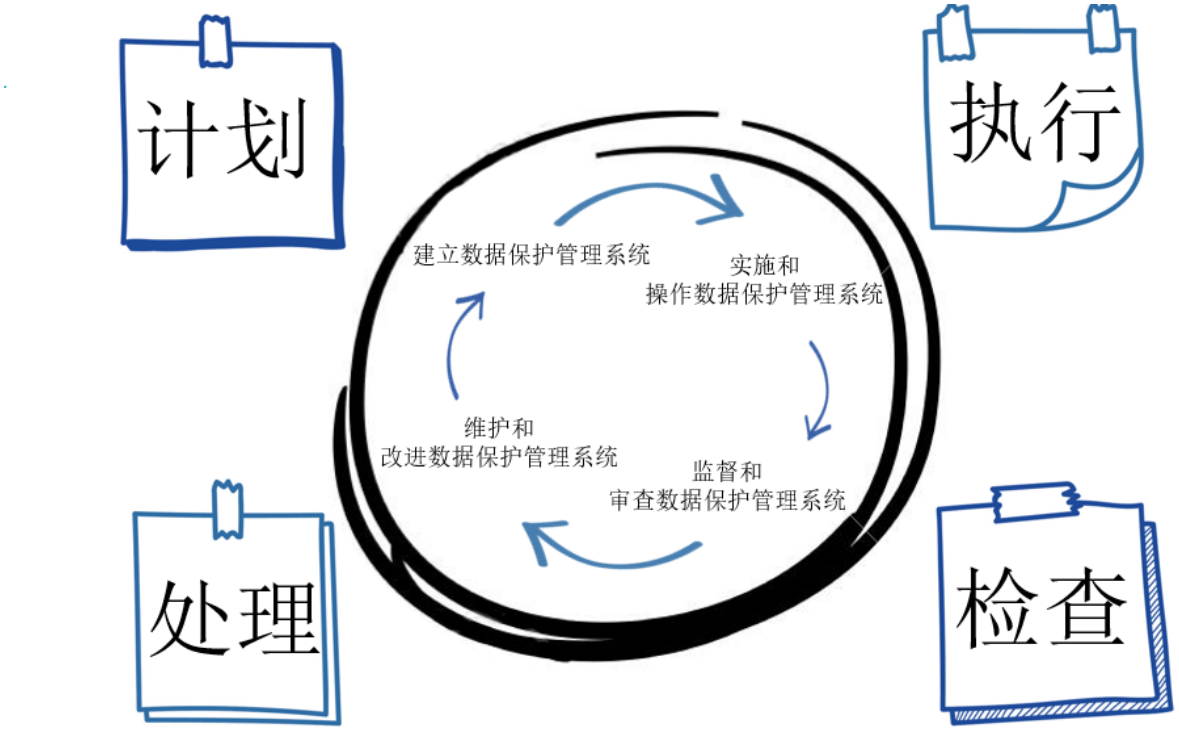
“**数据保护组织**主要由数据保护官、各个工厂及各个职能部门的协调员、首席执行官（数据控制方）、各个全球职能部门负责人（负责实施个人数据处理）及分包商（数据处理方）组成。”[MDPG001EN]

我们采用了一种流程化方式，建立、实施、操作、监督、审查、维护并改进罗盖特个人数据保护管理系统（**D**ata **P**rotection **M**anagement **S**ystem（**DPMS**））。

此治理中定义的个人数据保护管理流程和方式鼓励其用户强调以下方面的重要性：

1) 了解罗盖特的数据保护要求以及制定数据保护指令和程序的必要性；
2) 实施开展各项控制措施，在罗盖特的整体业务风险范围内管控罗盖特的数据保护风险；
3) 监督和考核数据保护管理系统的表现和成效；及
4) 基于客观衡量的持续改进。

我们采用“计划 – 执行 – 检查 – 处理”（PDCA）模型，该模型用于构建数据保护管理系统（DPMS）所有流程。



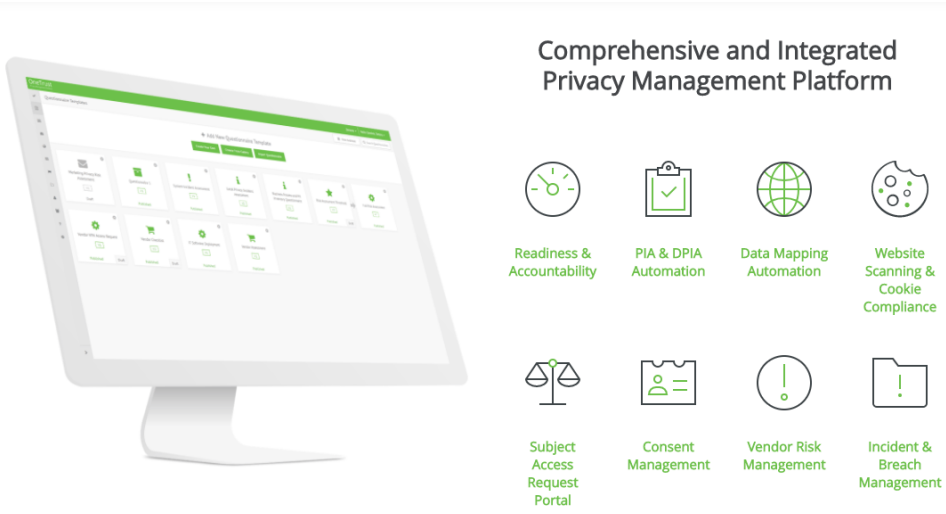
我们的方式：

我们的《通用数据保护条例》合规计划专注于：

- 了解我们企业如何收集、存储、使用和传输数据，确保做到合法合规；
- 在企业内部营造一种合规文化；
- 开展隐私影响评估；
- 为应对数据泄露做好准备；
- 将隐私计划的资源分配到位；
- 实施数据保护管理系统（计划－执行－检查－处理）。

为了实现这些目标，我们的隐私计划包括：

- 制定了数据保护政策以及相关的治理措施和文档；
- 管理《通用数据保护条例》合规项目，从而审查数据处理情况、管理数据泄露行为、审查合同、数据保护条款、数据传输协议等；
- 实施了符合《通用数据保护条例》的隐私管理软件。



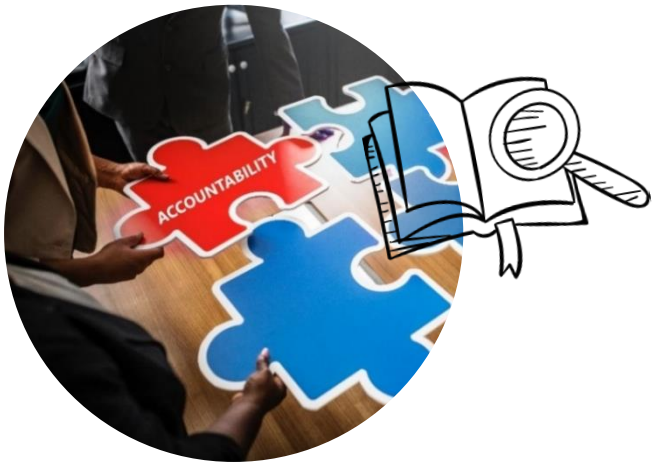
该管理平台的主要特色包括：

- 维护数据处理寄存器（数据映射）；
- 数据处理相关风险管理（由隐私影响评估等造成的风险）；
- 管理各种请求和权利（访问、更正、异议等）；
- 管理各种事件和数据泄露情况；
- 管理合规文档。

问责制

问责制是数据保护原则之一。它使我们有责任遵守《通用数据保护条例》，并规定我们必须能够证明自己的合规情况。

问责制为什么很重要？



我们对自己的个人数据处理方式承担责任，并证明已采取措施保护员工的权利，这不仅可以让我们更加合法合规，还使我们更具竞争优势。问责制是展示和证明我们如何尊重员工隐私的真正机会。这有助于我们培养并维持员工的信任感。

此外，如果确实出现问题，则能够表明我们积极考虑了各种风险并采取了各种措施和保障手段，有助于在面临潜在执法行动时降低我们的责任。另一方面，如果我们无法展示良好的数据保护做法，则可能使我们面临罚款和声誉受损的风险。

遵循问责制原则有什么实际意义？

个人数据处理需要小心谨慎，并应采取具体实用的保护措施。遵循责任制原则意味着：

- 记录并酌情传达与隐私相关的所有指令、程序及做法（“集团政策”）；
- 将集团政策实施任务分派给企业内指定的个人（他们继而酌情指派给企业内的其他人）；
- 在将个人数据传输给第三方时，确保第三方接收者有义务通过合同或强制性内部政策等其他手段，提供同等级别的隐私和数据保护（适用法律会包含有关国际数据传输的其他要求）；
- 为访问个人数据的数据控制方人员提供适当的培训；
- 建立有效的内部投诉处理和补救程序，供数据主体使用；
- 向数据主体告知可能会对其造成重大损害的隐私泄漏行为（除非被禁止，例如在配合执法部门时被禁止）以及采取的解决措施；

- 根据某些司法管辖机关（如数据保护机构）的要求以及风险级别，将隐私泄漏行为通知与隐私有关的所有利益相关者；
- 如果发生隐私泄漏行为，则允许受害的数据主体获得适当有效的制裁和/或补救措施，如纠正、删除或赔偿；
- 如果很难或无法使自然人的隐私状态恢复如初，则考虑启用补偿程序。

检查表：

☑ 我们要负起责任，确保最高管理层及整个组织都能遵守《通用数据保护条例》。
☑ 我们留存在遵守《通用数据保护条例》方面所采取的各项措施的证据。

我们制定了相应的技术措施和组织措施，如：

☑ 通过和实施数据保护规则；
☑ 采取“通过设计和默认方式实现数据保护”的方式——为我们数据处理操作的整个生命周期制定相应的数据保护措施；
☑ 与处理我们个人数据的代理方签订书面合同；
☑ 保留我们数据处理操作的书面记录；
☑ 实施相应的安全措施；
☑ 记录个人数据泄漏行为并在必要时报告；
☑ 对可能会对个人利益造成高风险的个人数据使用开展数据保护影响评估；
☑ 任命一名数据保护官；及
☑ 遵守相关的行为准则并签署认证计划（如可能）。

☑ 我们会适时定期审查和更新问责措施。

文档记录

什么是文档记录？

我们需要保留数据处理活动的记录，包括处理目的、数据共享和保留等方面；我们称之为**文档记录**。

记录我们的数据处理活动非常重要，不仅因为这本身就是一项法律要求，而且还因为这有助于实现良好的数据治理，有助于证明我们在《通用数据保护条例》及现行数据保护法律的其他方面的合规情况。

检查表：

数据处理活动的文档记录 – 要求

- ☑ 作为所处理的个人数据的控制方，我们记录了《通用数据保护条例》第 30（1）条规定的所有适用信息。
- ☑ 我们以书面形式记录数据处理活动。
- ☑ 我们以精细化方式记录数据处理活动，并在不同信息之间建立了有意义的联系。
- ☑ 我们会定期审查所处理的个人数据，并据此更新文档记录。

数据处理活动的文档记录 – 最佳做法

- ☑ 我们以电子形式记录数据处理活动，方便我们添加、删除及修改信息。

在准备记录数据处理活动时，我们：

- ☑ 进行信息审核，以了解我们的组织拥有哪些个人数据；
- ☑ 通过我们的数字化工具、安全工具及隐私工具开展问卷调查，并与全公司的员工交谈，从而更加全面地了解数据处理活动；及
- ☑ 审查集团政策、指令、程序、合同及协议，以解决数据保留、安全及数据共享等领域的问题。

我们的数据处理活动记录还包括记录以下信息或使其链接到文档记录：

- ☑ 隐私声明所需的信息；
- ☑ 必要时的同意记录；
- ☑ 数据控制方与处理方之间签订的合同；
- ☑ 个人数据的位置；
- ☑ 数据保护影响评估报告；及
- ☑ 个人数据泄露记录；
- ☑ 数据主体请求的记录。

我们的数据保护文档记录在哪里？

ONE
全球职能部门
数据保护

Privacy & Data Protection

“数据保护关乎集团的每位员工，人人有责”

内容

- 法律法规
- 信息与宣贯
- 最佳做法与政策

ONE
社群
数据保护网络

Data Protection Network

“我们人人都是个人数据保护的参与者”

内容

- 个人数据保护政策
- 数据保护管理系统
- 本地法规
- 人力资源
- 全球数字化
- 法务与合规
- 内部审计和控制
- 全球事业部与商业
- 创新研发
- 全球安保
- 保险与风险管理

OneTrust
隐私管理软件

OneTrust
Privacy Management Software
@ ROQUETTE

“专门针对隐私安全和第三方风险的隐私管理工具”

模块

文化 → 合规 → 问责制

隐私影响评估

隐私影响评估（**PIA**）这一流程旨在描述数据处理情况，评估数据处理的必要性和相称性，并通过评估和确定解决措施，帮助管理由于个人数据处理而导致的自然人权利和自由方面的风险。

首字母缩略词“**PIA**”可互换使用，指**隐私影响评估（Privacy Impact Assessment）**和**数据保护影响评估（Data Protection Impact Assessment）**（**DPIA**）。

如何开展隐私影响评估？

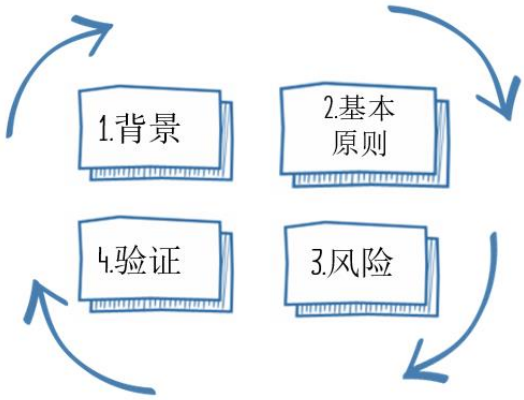
通过开展隐私影响评估实现合规性的方式基于两大支柱：

1) **基本权利和原则**，这些法律规定的权利和原则，无论其性质、严重性及风险程度如何，都必须予以尊重，“不容协商”；
2) **对数据主体的隐私风险进行管理**，从而确定相应的技术和组织控制措施来保护个人数据。

合规方式采用隐私影响评估

总而言之，开展隐私影响评估必须：

1) 确定和说明所考虑的个人数据处理的背景；
2) 分析保证遵守基本原则的控制措施：数据处理的相称性和必要性，以及对数据主体权利的保护；
3) 评估与数据安全相关的隐私风险，并确保风险得到妥善处理；
4) 基于要递交的以往情况说明或对以往步骤修改的决定，正式记录隐私影响评估的验证情况。



开展隐私影响评估的一般方法

这是一个持续改进的过程。因此，有时需要多次迭代才能建立符合要求的隐私保护系统。这个过程还需要定期（如一年一次）监控变化（在背景、控制措施、风险等方面的变化），并在发生重大变化时进行更新。

该方式应在新的个人数据处理流程设计好后立即实施。从一开始就采用这种方式可以确定必要充分的控制措施，从而优化成本。相反，在创建好系统并执行了控制措施后再实施这种方式可能会让人对做出的选择产生质疑。

我们的责任：

- 如果有一类数据处理专门采用新技术，将处理的性质、范围、背景及目的都考虑在内，但是有可能对自然人的权利和自由产生较高风险，则作为数据控制方的罗盖特，在处理数据之前，应对预期的处理操作开展个人数据保护影响评估。
- 在开展数据保护影响评估时，项目负责人应向指定的数据保护官员寻求建议。

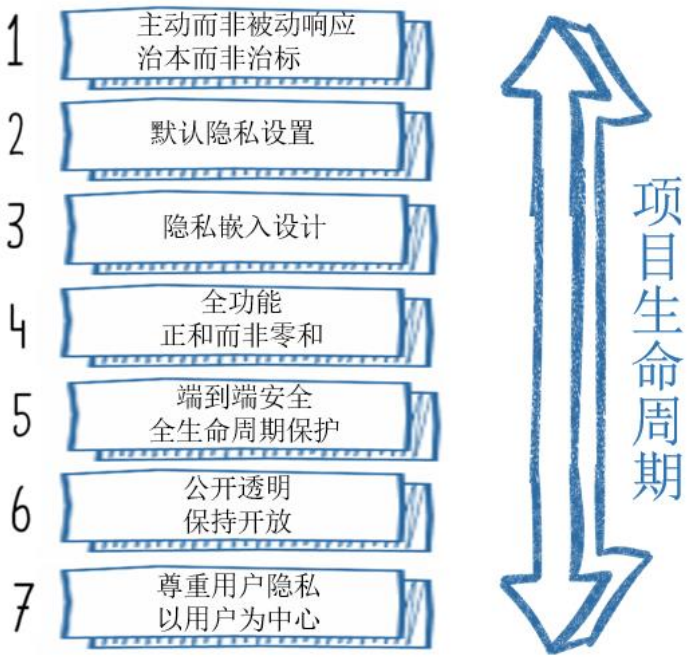
规则	Q-Docs 标准	《通用数据保护条例》标准
• 高风险情况下开展隐私影响评估	DDPG003EN 规则 1	第 35 条
• 隐私影响评估内容	DDPG003EN 规则 2	
• 数据保护官的隐私影响评估相关任务	DDPG003EN 规则 3	
• 隐私影响评估的审查	DDPG003EN 规则 4	

我们培训员工，改进内部流程。

- 学习 “Security & Privacy Review” 成 “Projects & Contracts”。
- 了解更多 ：法国国家信息与自由委员会隐私影响评估方法，2018 年 2 月版 - https://www.cnil.fr/en/home。

隐私设计和默认隐私

隐私设计指将隐私纳入特定的系统、业务流程或设计规范的设计、操作及管理中。



什么是通过设计保护数据？

数据保护法规包含维护数据主体隐私的基本原则。

通过设计以及默认方式进行数据保护，这有助于确保我们使用的信息系统满足这些数据保护原则，并确保这些系统维护数据主体的权利。

我们认为：

罗盖特依靠各种信息系统和数据库来执行一系列操作和管理任务。这些信息系统中有很大一部分都涉及到个人数据的处理，因此充分遵守该条例至关重要。

认真对待数据保护问题的企业可以建立信任。

因此，强大的数据保护措施可以成为企业的竞争优势。

管理层的投入对于做出这样的决定至关重要：在集团的采购和软件开发中，运用通过设计保护数据的原则。

管理层还必须确保为这项任务提供充足资源。

与对现有软件进行更改相比，在整个开发过程中将数据保护考虑在内不仅具有成本效益，而且效率更高。

我们的责任：

根据《通用数据保护条例》的规定，通过设计保护数据首次成为一项法律义务。这意味着数据保护和隐私必须内置于信息通信系统和技术的设计规范和体系结构中。

在软件开发期间以及在订购各种系统、解决方案和服务时，罗盖特作为数据控制方，必须遵守通过设计保护数据的各项相关要求。

因此，在与供应商达成协议或聘用顾问时，也必须相应地包括这些要求（请参阅我们的分包商标准）。

规则	Q-Docs 标准	《通用数据保护条例》标准
• 通过设计和默认方式实现安全、隐私及数据保护	DDPG007EN 规则 3	第 25 条

检查表：

- ☑ 审查数据保护影响评估（DPIA）
- ☑ 对敏感个人数据的收集和处理需求进行避免、限制或最小化
- ☑ 对用户界面中不必要的功能和个人数据的公开情况进行限制和最小化
- ☑ 尽可能对个人数据匿名化或假名化
- ☑ 默认情况下，所有隐私友好型配置都必须处于启用状态
- ☑ 默认情况下，应禁用从一个网站到另一个网站的跟踪
- ☑ 通过软件内的菜单撤回同意。请记住，如果撤回同意，则必须停止收集个人数据
- ☑ 设置应显示在菜单中，数据主体必须在此菜单中做出有意识的选择，主动“更改”对隐私不太友好的设置
- ☑ 默认情况下应禁用设备跟踪

我们培训员工，改进内部流程。

- 我们的社群“数据保护网络”上的指南。
- 方法：审查各个项目和合同的安全性与合规性。
- 在人力资源平台上学习。

数据泄漏通知

什么是个人数据泄露？

个人数据泄露是指违反安全措施，导致传输、存储或以其他方式处理的个人数据遭受意外销毁、非法销毁、丢失、更改、未经授权披露或访问的情况。

这意味着泄漏不仅仅指个人数据的丢失。

示例：

- 客户数据库丢失
- 员工绩效评估结果泄漏

我们的责任：

对于个人数据泄漏行为，我们必须依照规则办事，减少泄漏对数据主体的影响，并防止此类事件再次发生。

规则	Q-Docs 标准	《通用数据保护条例》标准
• 将个人数据泄露情况通知数据保护官。	DDPG008EN 规则 1	第 33 条
• 将个人数据泄露情况通知监管机构。	DDPG008EN 规则 2	
• 向数据主体传达个人数据泄露情况。	DDPG008EN 规则 3	第 34 条

发生数据泄露时我们应该联系谁？

请联系数据保护官：dpo@Roquette.com，以及罗盖特保密警报热线：alert@Roquette.com。

我们必须在多长时间内报告数据泄漏情况？

我们必须毫不迟延地向监管机构报告应该上报的泄漏情况，不得迟于知悉后 72 小时。

我们需要将哪些数据泄漏情况通知相关监管机构？

只有数据泄漏可能会损害个人权利和自由时，我们才需要通知相关监管机构。如果未得到解决，则此类数据泄漏行为可能会对个人产生重大不利影响。例如：

- 导致歧视；
- 声誉受损；
- 经济损失；或
- 失去机密性或其他任何重大的经济或社会劣势。

我们必须根据具体情况对此进行评估，并且需要对您的决定进行合理化证明，才能向监管机构举报数据泄漏情况。

我们什么时候必须通知个人？

如果违规行为可能给个人的权利和自由带来**高风险**，我们必须毫不犹豫地直接通知相关人员。

如发生以下情形，则无义务将数据泄漏情况通知个人：

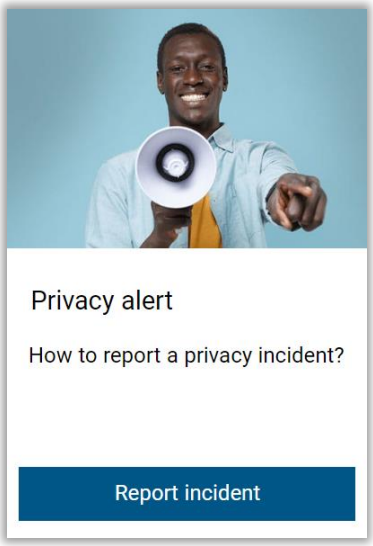
- 我们已实施了相应的技术措施和组织措施，这些措施适用于受泄漏影响的个人数据；
- 我们已采取后续措施，以确保不再可能对个人的权利和自由造成任何高风险；或
- 这需要付出不合常理的努力。

如果传达数据泄漏情况需要付出不合常理的努力，则我们必须以另一种同样有效的方式将信息提供给个人，如公开传达。

如果发生数据泄露，我们应该联系谁？

请联系数据保护官（dpo@Roquette.com ）
和/或通过我们的 "Privacy Alert" 网络表格报告事件。

如果您需要报告潜在的违规行为，
可以与您的常规联系人联系，或通过保密的 Roquette 警报设备报告问题： Speakup©.



监督与审查

我们认为：

罗凯特致力于：

☑ 确保对数据保护要求进行合法的技术**监督**；

☑ **审查**并**改进**我们的数据保护管理系统（DPMS）

从而将法规更新情况和技术进展以及内部服务约束考虑在内。[DDPG009EN]

我们的责任：

规则	Q-Docs 标准	《通用数据保护条例》标准
• 确保对个人数据保护开展合法的技术监督与审查	DDPG009EN 规则 1	最佳做法
• 定期监督数据保护管理系统和数据保护指令的实施情况	DDPG009EN 规则 2	
• 定期审查个人数据保护政策和数据保护管理系统文档	DDPG009EN 规则 3	

在人力资源平台上学习。

设计并支持我们的隐私计划

法规研究软件：

我们使用的平台可以提供一系列隐私解决方案，旨在帮助我们监督法规更新情况，降低风险并实现全球范围的合规性：

- ☑ 法规跟踪
- ☑ 跨境比较图
- ☑ 指导说明
- ☑ 《通用数据保护条例》门户网站
- ☑ 模板和检查表
- ☑ 要求分析师提供服务
- ☑ 法律研究

数据保护管理系统的审计和审查：

我们开展内部审计，以确定数据保护管理系统的输入内容是否：

- ☑ 符合本指南、集团政策及适用法律法规的要求；
- ☑ 得到有效实施和维护；及
- ☑ 符合预期表现。

我们对数据保护管理系统开展管理审查，以确保系统范围仍然足够，并确定数据保护管理系统流程中需要改进的地方。

为此，输入内容应包括：

- ☑ 数据保护管理系统的目标、控制措施、流程及程序；
- ☑ 以往的合规审计和控制措施的结果；
- ☑ 有关方面的反馈；
- ☑ 可以在集团中用来改进数据保护管理系统绩效和成效的技术、产品或程序；
- ☑ 预防措施和纠正措施的状况；
- ☑ 在以往的风险评估中未得到充分解决的漏洞或威胁；
- ☑ 成效衡量结果；
- ☑ 以往管理审查的跟进行动；
- ☑ 任何可能影响数据保护管理系统的更改；及
- ☑ 改进建议。

参考文件

- [《行为守则》]罗盖特集团行为守则
- [GDPG001EN]与数据保护有关的各项定义术语表
- [MDPG001EN]个人数据保护手册
- [DDPG001EN]尊重隐私和数据保护文化指令
- [DDPG002EN]个人数据处理合法性指令
- [DDPG003EN]隐私影响评估指令
- [DDPG004EN]敏感数据处理指令
- [DDPG005EN]处理活动记录指令
- [DDPG006EN]尊重人员权利指令
- [DDPG007EN]个人数据安全指令
- [DDPG008EN]个人数据泄漏通知指令
- [DDPG009EN]个人数据管理系统审查指令
- [DSUG001EN]信息保护指令
- [DSUG006EN]网络安全管理指令
- [DSUG016EN]承包商安全指令

参考书目

[《欧盟宪章》]《欧盟基本权利宪章》，2010/C 83/02。

[《通用数据保护条例》]欧洲议会和欧洲理事会于 2016 年 4 月 27 日颁布的欧盟第 2016/679 号条例，内容是关于在处理个人数据和此类数据自由流通方面对自然人的保护，同时废除 95/46/EC 指令（《通用数据保护条例》）。

[《数据保护法》]《法国数据保护法》，1978 年 1 月 6 日第 78－17 号法案 25 号修正案。

[第 29 条工作小组指南]关于确定数据控制方或处理方领导监管机构的指南| WP 244 号指南修订版 01（2017 年 4 月 5 日）。

[第 29 条工作小组指南]关于在实施第 2016/679 号条例时开展数据保护影响评估（DPIA）及确定数据处理是否“可能导致高风险”的指南| WP 248 号指南修订版 01（2017 年 10 月 13 日）。

[第 29 条工作小组指南]关于在实施第 2016/679 号条例时行政罚款的运用和设定指南| WP 253 号指南（2017 年 10 月 21 日）。

[第 29 条工作小组指南]关于在实施第 2016/679 号条例时自动化个人决策和剖析的指南| WP 251 号指南修订版 01（2018 年 2 月 13 日）。

[第 29 条工作小组指南]关于数据保护官（“DPO”）的指南| WP 243 号指南修订版 01（2017 年 4 月 5 日）。

[第 29 条工作小组指南]关于第 2016/679 号条例透明度条款的指南| WP260 号指南修订版 01（2018 年 4 月 11 日）。

[第 29 条工作小组指南]关于第 2016/679 号条例同意条款的指南| WP259 号指南修订版 01（2018 年 4 月 11 日）。

[欧盟数据保护委员会意见]关于刑事事项电子证据的制作和保存令的委员会提案第 23/2018 号意见（第 70.1.b 条）（2018 年 9 月 26 日）。

[欧盟数据保护委员会意见]关于在日本实施个人数据充分保护决定的欧盟委员会草案第 28/2018 号意见（2018 年 12 月 5 日）。

[欧盟数据保护委员会意见]关于 DK SA 提交的标准合同条款草案的第 14/2019 号意见（《通用数据保护条例》第 28（8）条）（2019 年 7 月 12 日）。

[欧盟数据保护委员会建议]关于受数据保护影响评估要求约束的数据处理操作的欧洲数据保护监管机构名单草案第 01/2019 号建议（欧盟第 2018/1725 号条例第 39（4）条）（2019 年 7 月 10 日）。

[欧盟数据保护委员会－欧洲数据保护专员公署共同回复]欧盟数据保护委员会－欧洲数据保护专员公署对公民自由、司法与内政事务委员会关于美国《澄清境外合法使用数据法案》对欧洲个人数据保护法律框架的影响的共同回复（附件）（2019 年 7 月 10 日）。

[欧盟数据保护委员会意见]关于免除数据保护影响评估要求的数据处理操作所涉及的法国主管监管机构名单草案第 13/2019 号意见（《通用数据保护条例》第 35（5）条）（2019 年 7 月 10 日）。

资料来源

- 法国国家信息与自由委员会
  - https://www.cnil.fr/en/home
  - 2019 年 9 月
  - 许可：CC-BY-ND 3.0 FR
- 英国信息专员办公室
  - https://ico.org.uk/
  - 2019 年 9 月
  - 根据开放政府许可协议发放许可
- 欧盟
  - https://eur-lex.europa.eu
  - 1998-2019 年
- https://www.iso.org/home.html
- https://www.dataguidance.com/
- https://www.onetrust.com/
- https://www.corporatefiction.fr/
- https://pixabay.com/fr/service/license/

本《指南》英文版仅作参考。
本文档译文可能需要解释。
第一版：2019 年 9 月
由罗盖特集团发布
编辑设计和图片：合规办公室
照片：随意使用

仅限内部使用。

ROQUETTE

Offering the best of nature™