Data Breach Event Response Framework	**数据泄露事件响应框架**
The GDPR defines a personal data breach as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.” (Article 4(12)).	根据《一般数据保护条例》（GDPR）中的定义，个人数据泄露是指“违反安全规定，导致传输、存储或以其他方式处理的个人数据意外或非法损毁、丢失、篡改、非授权披露或访问。”（第 4(12) 条）。
The following document outlines the step-by-step framework for how [Company Name], when acting as Data Controller, will handle a personal data breach. It is to be used in conjunction with the Data Event Report in which specific details of the breach will be outlined, as well as the remedial measures taken to minimise the risk to data subjects.	以下文件概述了 [公司名称] 作为数据控制者处理个人数据泄露的分步框架。本框架与数据事件报告一同使用，后者概述了具体的泄露信息以及为使数据主体风险最小化而采取的补救措施。
Discovery Phase	**发现阶段**
Step 1: Data breach occurs.	步骤 1：发生数据泄露。
Step 2a: Data breach is discovered by an internal or external source.	步骤 2a：内部或外部来源发现数据泄露。
Step 2b: Internal source reports the data breach to the Data Event Coordinator, [insert name here].	步骤 2b：内部来源将数据泄露报告给数据事件协调员 [此处插入姓名]。
Step 2c: External source reports the data breach to an internal source at [Company Name] by contacting [e.g. privacy@[Company Name].com] and that internal source reports the data breach to the Data Event Coordinator.	步骤 2c：外部来源通过联系 [例如：privacy@[Company Name].com] 将数据泄露报告给 [公司名称] 的内部来源，然后内部来源将数据泄露报告给数据事件协调员。
Step 2d: The Data Event Coordinator completes a preliminary version of the Data Event Report.	步骤 2d：数据事件协调员完成初版数据事件报告。
Reporting Phase	**报告阶段**
Step 3a: All relevant [Company Name] employees are to be interviewed about their knowledge of the data breach in order to gather as much information about the event as possible.	步骤 3a：与所有相关 [公司名称] 员工面谈，根据他们对数据泄露的了解，尽可能多地收集事件相关信息。
Step 3b: The Data Event Coordinator, together with [Company Name]’s IT team and relevant employees, shall continue gathering facts about the data breach in order to find its source.	步骤 3b：数据事件协调员以及 [公司名称] 的 IT 团队和相关员工应持续收集有关数据泄露的事实，从而找到其源头。
Step 4a: Under the GDPR, there is an obligation to report the data breach to the relevant Supervisory Authority. This shall be done within 72 hours of the time of discovery of the data breach.	步骤 4a：根据 GDPR 的规定，向相关监管机构报告数据泄露是一项义务。该报告必须在发现数据泄露后 72 小时内完成。

Step 4b: The data breach notification to the Supervisory Authority shall include the following information: description of the nature of the personal data breach; categories of data affected; the number of persons affected by the violation; the name and contact details of the point of contact from whom additional information can be obtained; specifics on the measures taken or to be taken to remedy the breach including, where appropriate, measures taken to mitigate negative consequences.	步骤 4b：向监管机构发出的数据泄露通告应包括以下信息：个人数据泄露性质说明；受影响数据类别；受违规影响的人数；可提供额外信息的联系人的姓名和联系方式；针对泄露事件已采取或拟采取的措施详情，包括（如恰当）减轻不利影响的措施。
Step 4c: Any new information gained after the report has been submitted to the Supervisory Authority, shall also be submitted to the Authority as soon as discovered.	步骤 4c：向监管机构提交报告后获得的任何新信息也须在发现后尽快交给监管机构。
Step 5: Where the data breach causes a high risk for data subjects, the data controllers may also have to inform, in simple and clear terms, the users affected by the incident, unless the controller has taken prior or subsequent technical or organisational measures. In this instance, the Data Event Coordinator, together with [Company Name]'s legal counsel, shall draft a notice that complies with these notification obligations. The Supervisory Authority will advise on whether such a communication shall be released to data subjects, based on an assessment of the risk incurred.	步骤 5：如果数据泄露对数据主体造成较高风险，数据控制者还必须简洁明了地告知受该事件影响的用户，除非控制者已经采取事前或事后技术或组织措施。在这类情况中，数据控制者以及 [公司名称] 的法律顾问应起草一份符合这些通告义务的声明。关于是否应向数据主体发布该声明，监管机构会在评估所产生的风险后提供建议。
Recovery Phase	**恢复阶段**
Step 5a: The [Company Name] security and IT team shall address the network security issues raised by the data breach and ensure the security of data in light of the event.	步骤 5a：[公司名称] 安全和 IT 团队应解决数据泄露导致的网络安全问题，并针对事件确保数据安全。
Step 5b: The Data Event Coordinator and [Company Name] senior management shall determine corrective actions for employees who may have contributed to the Data Event.	步骤 5b：数据事件协调员和 [公司名称] 高层管理人员应确定须对可能导致数据事件的员工采取的纠正措施。
Step 6: The Data Event Coordinator shall finalise the Data Event Report, including post-event follow up items, and including any and all relevant facts related to the data breach. The Report shall be documented and stored for evidence and reference.	步骤 6：数据事件协调员应最终敲定数据事件报告，其中涵盖事后跟进项目，包括与数据泄露相关的任何及所有事实。报告应形成文件并妥善保管，作为证据和参考。
Step 7: [Company Name] shall implement all remedial actions to minimise the impact of the data breach.	步骤 7：[公司名称] 应实施各项补救措施，最大程度地降低数据泄露的影响。