**Privacy and Data Protection II**

**一、公平信息原则（Fair Information Principles, FIPs）**

FIPs 是《通用数据保护条例》（GDPR）和隐私保护的核心原则，指导如何合法、公平地处理个人数据。以下是具体原则的详细解释及条文中英对照。

**1. 合法和公平处理（Fair and Lawful Processing）**

**1.1 原则内容**

个人数据的处理必须符合法律规定，并确保数据主体知情与同意。数据控制者必须透明地向数据主体说明数据的处理目的和方式。

**1.2 相关条文**

**GDPR 第 5(1)(a) 条**

“Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.”  
**“个人数据应以合法、公平和透明的方式处理。”**

**GDPR 第 6(1) 条**

“Processing shall be lawful only if and to the extent that at least one of the following applies…”  
**“处理只有在至少满足以下条件之一时才是合法的……”**

具体合法处理基础包括：

* **(a) 同意（Consent）**

“The data subject has given consent to the processing of his or her personal data for one or more specific purposes.”  
**“数据主体已就其个人数据的一个或多个特定目的的处理给予同意。”**

* **(b) 合同履行（Contract）**

“Processing is necessary for the performance of a contract to which the data subject is party.”  
**“为履行数据主体参与的合同所必须的处理。”**

* **(c) 法律义务（Legal Obligation）**

“Processing is necessary for compliance with a legal obligation to which the controller is subject.”  
**“为履行控制者承担的法律义务所必须的处理。”**

* **(d) 保护重要利益（Vital Interests）**

“Processing is necessary in order to protect the vital interests of the data subject or of another natural person.”  
**“为保护数据主体或其他自然人的重要利益所必须的处理。”**

**2. 比例性原则（Proportionality Principle）**

**2.1 原则内容**

数据的处理应确保与处理目的相关、适当，不得超出必要的范围。这要求数据收集者只收集与目的密切相关的数据，并避免处理与目的无关的额外数据。

**2.2 相关条文**

**GDPR 第 5(1)(c) 条**

“Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.”  
**“个人数据应当适度、相关，并限于为实现处理目的所必须的范围。”**

这一原则确保处理的数据不会过多，从而降低数据泄露和误用的风险。

**3. 最小化原则（Minimality Principle）**

**3.1 原则内容**

最小化原则要求数据控制者在收集和存储个人数据时，只保留实现特定合法目的所必需的数据。一旦数据不再必要，应及时删除。

**3.2 相关条文**

**GDPR 第 5(1)(c) 条**

“Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.”  
**“个人数据应当适度、相关，并限于为实现处理目的所必须的范围。”**

此外，数据控制者需制定数据保留期限，避免数据长期存储造成隐私风险。

**4. 目的限制原则（Purpose Limitation Principle）**

**4.1 原则内容**

收集的个人数据只能用于明确、合法的特定目的。若要将数据用于其他目的，则需确保新目的与原始目的兼容或获得数据主体的额外同意。

**4.2 相关条文**

**GDPR 第 5(1)(b) 条**

“Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.”  
**“个人数据应为明确、合法的特定目的而收集，不得以与这些目的不相符的方式进一步处理。”**

但有以下例外：

* **科学研究、统计目的**

“Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes.”  
**“为公共利益的档案目的、科学或历史研究目的或统计目的进一步处理数据，不视为与最初目的不相符。”**

**5. 数据主体影响力（Data Subject Influence）**

**5.1 原则内容**

数据主体有权参与其个人数据的处理，并对数据处理过程施加一定的影响。这包括以下具体权利：

* **知情权（Right to be informed）**  
  数据主体有权了解其数据的用途、存储方式及存储期限。
* **访问权（Right of access）**  
  数据主体可以请求访问其个人数据副本。
* **更正权（Right to rectification）**  
  数据主体有权要求更正不准确或不完整的数据。
* **删除权（Right to erasure, 又称“被遗忘权”）**  
  数据主体在某些条件下有权要求删除其个人数据。

**5.2 相关条文**

**GDPR 第 12-23 条**

“The data subject shall have the right to access, rectify, erase and restrict the processing of their personal data.”  
**“数据主体有权访问、更正、删除其个人数据，并限制其数据的处理。”**

**6. 数据质量（Data Quality）**

**6.1 原则内容**

数据的准确性和及时更新对于保护数据主体权益至关重要。数据控制者必须确保存储的个人数据是正确的，并在必要时更新数据。

**6.2 相关条文**

**GDPR 第 5(1)(d) 条**

“Personal data shall be accurate and, where necessary, kept up to date.”  
**“个人数据应当准确，并在必要时保持更新。”**

* 如果发现数据不准确，应立即更正或删除。
* 确保处理的数据始终与原始目的相关，避免不必要的数据存储。

**7. 数据安全（Data Security）**

**7.1 原则内容**

数据安全要求保护个人数据免受未经授权的访问、丢失、损毁或修改。控制者和处理者必须采取适当的技术和组织措施，确保数据的**完整性（integrity）和保密性（confidentiality）**。

**7.2 相关条文**

**GDPR 第 5(1)(f) 条**

“Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.”  
**“个人数据应以确保适当安全的方式处理，包括防止未经授权或非法处理，以及意外丢失、破坏或损坏。”**

**GDPR 第 32 条**

“The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.”  
**“控制者和处理者应实施适当的技术和组织措施，以确保与风险相适应的安全水平。”**

具体措施包括：

* 数据加密（Encryption）
* 定期测试和评估安全措施的有效性
* 访问权限管理（Access control）

**8. 敏感性（Sensitivity）**

**8.1 原则内容**

某些类别的数据被归类为**敏感数据（Sensitive Data）**，需要特殊保护。这些数据可能揭示种族或民族出身、政治观点、宗教或哲学信仰等。

**8.2 相关条文**

**GDPR 第 9(1) 条**

“Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs… shall be prohibited.”  
**“处理揭示种族或民族出身、政治观点、宗教或哲学信仰等个人数据是被禁止的。”**

例外情况包括：

* 数据主体明确同意
* 处理与就业法、社会保障法相关的敏感数据
* 为保护数据主体或他人的生命所必须

此外，**基因数据（Genetic Data）**、\*\*生物识别数据（Biometric Data）\*\*等也属于敏感数据。

**二、个人数据、匿名数据和伪匿名数据的详细解释**

根据《通用数据保护条例》（GDPR），**个人数据**、**匿名数据**和**伪匿名数据**的定义和处理要求有所不同。以下是对这些概念的详细解释及相关条文中英对照。

**1. 个人数据（Personal Data）**

**1.1 定义**

**GDPR 第 4(1) 条**

“‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”  
**“‘个人数据’是指与已识别或可识别的自然人（‘数据主体’）相关的任何信息；可识别的自然人是可以通过直接或间接方式确定身份的个人，尤其是通过姓名、身份识别号码、位置数据、在线标识符或该自然人特有的身体、生理、基因、心理、经济、文化或社会身份的一个或多个因素来确定身份。”**

**1.2 处理要求**

* 处理个人数据必须符合**合法性、透明性、公平性**（GDPR 第 5 条）。
* 必须基于明确的法律基础，例如数据主体同意、合同履行等（GDPR 第 6 条）。
* 数据主体享有**知情权、访问权、删除权等权利**（GDPR 第 12-23 条）。

**2. 匿名数据（Anonymous Data）**

**2.1 定义**

**GDPR 序言第 26 段**

“The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.”  
**“数据保护原则不适用于匿名信息，即不与已识别或可识别的自然人相关的信息，或以使数据主体无法或不再被识别的方式匿名化的个人数据。”**

**2.2 处理要求**

* 匿名数据不受 GDPR 的约束，因为它无法与特定的个人建立联系。
* 主要用于统计、科学研究和公共政策制定等（GDPR 第 89 条）。

**2.3 匿名化与去识别化**

* **匿名化（Anonymization）**：一种使数据无法再与数据主体关联的技术。匿名化的关键在于**不可逆性**。
* **去识别化（De-identification）**：减少数据与数据主体关联的技术，但可能具有一定的**可逆性**。

**3. 伪匿名数据（Pseudonymous Data）**

**3.1 定义**

**GDPR 第 4(5) 条**

“‘Pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.”  
**“‘伪匿名化’是指通过特定方式处理个人数据，使个人数据在不使用附加信息的情况下，无法归属于特定的数据主体；并且此类附加信息应单独存储，并受技术和组织措施的保护，以确保个人数据无法归属于已识别或可识别的自然人。”**

**3.2 处理要求**

* **伪匿名数据仍属于个人数据**，因此受 GDPR 保护。
* 可以降低数据泄露风险，但需要采取严格的技术和组织措施来保护伪匿名化信息（GDPR 第 32 条）。
* 在某些情况下，伪匿名化可减少对数据主体权利的限制，例如**访问权和数据携带权**（GDPR 第 11 条）。

**3.3 与加密的关系**

**GDPR 序言第 28 段**

“Pseudonymisation can reduce the risks to the data subjects and help controllers and processors to meet their data protection obligations.”  
**“伪匿名化可以降低数据主体的风险，并帮助控制者和处理者履行其数据保护义务。”**

**4. 三者的比较**

| **类别** | **定义** | **GDPR 适用性** | **处理要求** |
| --- | --- | --- | --- |
| **个人数据** | 能直接或间接识别自然人的信息 | 完全适用 | 符合法律基础、透明性和数据主体权利 |
| **匿名数据** | 无法识别特定自然人的信息 | 不适用 | 无特别要求，用于研究和统计等 |
| **伪匿名数据** | 通过附加信息才能识别的个人数据 | 完全适用 | 必须有技术和组织措施保护，仍需遵守 GDPR 原则 |

**三、数据泄露的详细解释**

根据《通用数据保护条例》（GDPR），数据泄露的管理是数据保护的重要组成部分，包括**数据泄露的定义**、**通知义务**和**可能的罚款**。以下是对这些内容的详细解释及相关条文中英对照。

**1. 数据泄露的定义（Definition of Data Breach）**

**1.1 定义**

**GDPR 第 4(12) 条**

“Personal data breach means 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.”  
**“个人数据泄露是指因安全漏洞导致的个人数据在传输、存储或其他处理过程中被意外或非法破坏、丢失、更改、未经授权披露或访问。”**

**1.2 数据泄露的类型**

* **机密性泄露（Confidentiality breach）**：未经授权的访问或披露。
* **完整性泄露（Integrity breach）**：数据被意外或恶意更改。
* **可用性泄露（Availability breach）**：数据意外丢失或无法访问。

**2. 数据泄露的通知义务（Notification Obligations）**

**2.1 向监督机构的通知（Notification to Supervisory Authority）**

**GDPR 第 33 条**

“In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority…”  
**“在发生个人数据泄露的情况下，控制者应毫不拖延，并在得知泄露后 72 小时内（如可行）通知监督机构……”**

* **通知内容要求（Article 33(3)）**：  
  通知需至少包括以下内容：
  + 数据泄露的性质、受影响的数据类别和记录数量。

“Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.”  
**“描述个人数据泄露的性质，包括（如可能）受影响的数据主体类别和大致数量，以及个人数据记录的类别和大致数量。”**

* + 数据保护官（DPO）或其他联系人的信息。
  + 数据泄露可能的后果。
  + 控制者已采取或计划采取的应对措施。

**2.2 向数据主体的通知（Notification to Data Subjects）**

**GDPR 第 34 条**

“When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.”  
**“如果个人数据泄露可能对自然人的权利和自由构成高风险，控制者应毫不拖延地将泄露信息告知数据主体。”**

* **内容要求**：包括泄露的性质、控制者的联系方式、建议的数据保护措施。

**2.3 例外情况**

如果控制者已采取适当技术和组织措施（如加密），或者确保泄露不会对数据主体造成高风险，则无需通知数据主体。

**3. 可能的罚款（Possible Fines）**

**GDPR 第 83 条**  
根据违规的严重程度，GDPR 将罚款分为两个等级：

**3.1 较低等级的罚款**

“Up to 10,000,000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.”  
**“最高可处以 1,000 万欧元，或（如为企业）上一财年全球年度总营业额的 2%，以较高者为准。”**

**3.2 较高等级的罚款**

“Up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.”  
**“最高可处以 2,000 万欧元，或（如为企业）上一财年全球年度总营业额的 4%，以较高者为准。”**

**3.3 决定罚款金额的因素**

罚款金额的确定取决于以下因素（Article 83(2)）：

* 违规的性质、严重程度和持续时间。
* 控制者是否采取措施减轻数据主体的损害。
* 违规是否故意或由于疏忽导致。
* 控制者的历史违规记录。

**关键点总结**

1. **数据泄露的定义**包括安全漏洞导致的破坏、丢失、篡改、未经授权的披露或访问。
2. **通知义务**要求在 72 小时内通知监督机构，在高风险情况下通知数据主体。
3. **可能的罚款**根据违规的严重程度分为两级，最高可达企业年度总营业额的 4%。

**数据泄露的详细解释**

根据《通用数据保护条例》（GDPR），数据泄露的管理是数据保护的重要组成部分，包括**数据泄露的定义**、**通知义务**和**可能的罚款**。以下是对这些内容的详细解释及相关条文中英对照。

**1. 数据泄露的定义（Definition of Data Breach）**

**1.1 定义**

**GDPR 第 4(12) 条**

“Personal data breach means 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.”  
**“个人数据泄露是指因安全漏洞导致的个人数据在传输、存储或其他处理过程中被意外或非法破坏、丢失、更改、未经授权披露或访问。”**

**1.2 数据泄露的类型**

* **机密性泄露（Confidentiality breach）**：未经授权的访问或披露。
* **完整性泄露（Integrity breach）**：数据被意外或恶意更改。
* **可用性泄露（Availability breach）**：数据意外丢失或无法访问。

**2. 数据泄露的通知义务（Notification Obligations）**

**2.1 向监督机构的通知（Notification to Supervisory Authority）**

**GDPR 第 33 条**

“In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority…”  
**“在发生个人数据泄露的情况下，控制者应毫不拖延，并在得知泄露后 72 小时内（如可行）通知监督机构……”**

* **通知内容要求（Article 33(3)）**：  
  通知需至少包括以下内容：
  + 数据泄露的性质、受影响的数据类别和记录数量。

“Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.”  
**“描述个人数据泄露的性质，包括（如可能）受影响的数据主体类别和大致数量，以及个人数据记录的类别和大致数量。”**

* + 数据保护官（DPO）或其他联系人的信息。
  + 数据泄露可能的后果。
  + 控制者已采取或计划采取的应对措施。

**2.2 向数据主体的通知（Notification to Data Subjects）**

**GDPR 第 34 条**

“When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.”  
**“如果个人数据泄露可能对自然人的权利和自由构成高风险，控制者应毫不拖延地将泄露信息告知数据主体。”**

* **内容要求**：包括泄露的性质、控制者的联系方式、建议的数据保护措施。

**2.3 例外情况**

如果控制者已采取适当技术和组织措施（如加密），或者确保泄露不会对数据主体造成高风险，则无需通知数据主体。

**3. 可能的罚款（Possible Fines）**

**GDPR 第 83 条**  
根据违规的严重程度，GDPR 将罚款分为两个等级：

**3.1 较低等级的罚款**

“Up to 10,000,000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.”  
**“最高可处以 1,000 万欧元，或（如为企业）上一财年全球年度总营业额的 2%，以较高者为准。”**

**3.2 较高等级的罚款**

“Up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.”  
**“最高可处以 2,000 万欧元，或（如为企业）上一财年全球年度总营业额的 4%，以较高者为准。”**

**3.3 决定罚款金额的因素**

罚款金额的确定取决于以下因素（Article 83(2)）：

* 违规的性质、严重程度和持续时间。
* 控制者是否采取措施减轻数据主体的损害。
* 违规是否故意或由于疏忽导致。
* 控制者的历史违规记录。

**关键点总结**

1. **数据泄露的定义**包括安全漏洞导致的破坏、丢失、篡改、未经授权的披露或访问。
2. **通知义务**要求在 72 小时内通知监督机构，在高风险情况下通知数据主体。
3. **可能的罚款**根据违规的严重程度分为两级，最高可达企业年度总营业额的 4%。

如需进一步探讨或分析具体案例，请告诉我！

4o

**您说：**

数据控制者和处理者的角色 控制者与处理者的责任划分及其义务 仔细解释，列出条文，中英对照

**ChatGPT 说：**

ChatGPT

**四、数据控制者和处理者的角色**

在《通用数据保护条例》（GDPR）中，数据控制者（Controller）和数据处理者（Processor）的角色、责任和义务有明确的划分。以下是详细解释及相关条文中英对照：

**1. 数据控制者（Controller）的定义与责任**

**1.1 定义**

**GDPR 第 4(7) 条**

“‘Controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.”  
**“‘控制者’是指单独或与他人共同决定个人数据处理目的和方式的自然人或法人、公共机构、代理机构或其他机构。”**

**1.2 控制者的主要责任**

控制者对个人数据的处理活动负有主要责任，必须确保其活动符合 GDPR 的要求。

**GDPR 第 24 条：责任原则（Responsibility Principle）**

“The controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.”  
**“控制者应实施适当的技术和组织措施，以确保并能够证明数据处理符合本条例。”**

**具体责任包括：**

1. **确保合法性、透明性和目的限制（Article 5 GDPR）**  
   控制者需遵守 GDPR 中关于数据处理的基本原则。
2. **提供数据主体权利（Article 12-23 GDPR）**
   * 控制者需确保数据主体能够行使其权利，如访问权、更正权、删除权等。
3. **数据保护影响评估（Data Protection Impact Assessment, DPIA, Article 35 GDPR）**
   * 在高风险情况下，控制者需进行 DPIA，以评估数据处理的潜在影响。
4. **通知数据泄露（Article 33 GDPR）**
   * 如果发生数据泄露，控制者需在 72 小时内通知监督机构。

**2. 数据处理者（Processor）的定义与责任**

**2.1 定义**

**GDPR 第 4(8) 条**

“‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.”  
**“‘处理者’是指代表控制者处理个人数据的自然人或法人、公共机构、代理机构或其他机构。”**

**2.2 处理者的主要责任**

数据处理者按照控制者的指示处理数据，但也需要确保其活动符合 GDPR 的要求。

**GDPR 第 28 条：处理者的义务（Processor Obligations）**

“The processor shall not engage another processor without prior specific or general written authorisation of the controller.”  
**“未经控制者的事先具体或一般书面授权，处理者不得委托其他处理者。”**

**具体责任包括：**

1. **按控制者指示处理数据（Article 28(3) GDPR）**
   * 处理者仅能根据控制者明确指示处理数据。
2. **数据安全（Article 32 GDPR）**
   * 处理者需采取技术和组织措施保护数据安全。
3. **数据泄露通知（Article 33 GDPR）**
   * 一旦发生数据泄露，处理者需及时通知控制者。
4. **记录处理活动（Records of Processing Activities, Article 30 GDPR）**
   * 处理者需维护其数据处理活动的记录，以备监督机构审查。

**3. 控制者与处理者的共同责任**

**3.1 联合控制者（Joint Controllers）**

**GDPR 第 26 条**

“Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.”  
**“当两个或多个控制者共同决定数据处理的目的和方式时，他们应视为联合控制者。”**

* 联合控制者需明确彼此的责任分工，并通过协议约定数据主体权利的行使方式。

**3.2 处理协议（Processing Agreement）**

**GDPR 第 28(3) 条**

“Processing by a processor shall be governed by a contract or other legal act under Union or Member State law.”  
**“处理者对数据的处理应受欧盟或成员国法律规定的合同或其他法律行为的约束。”**

* 控制者与处理者之间必须签订数据处理协议，明确处理者的义务和责任。

**4. 罚款与法律后果**

**4.1 控制者的罚款**

* 如果控制者未履行其义务，可能面临 GDPR 第 83 条规定的罚款，最高可达**2,000 万欧元或全球营业额的 4%**。

**4.2 处理者的罚款**

* 处理者如未履行数据安全或按控制者指示处理数据的义务，也可能面临相同级别的罚款。

**总结表**

| **角色** | **定义** | **主要责任** |
| --- | --- | --- |
| **控制者** | 决定数据处理目的和方式 | 1. 确保数据处理符合 GDPR 要求 2. 负责数据泄露通知 3. 提供数据主体权利 4. 进行数据保护影响评估 |
| **处理者** | 代表控制者处理数据 | 1. 按控制者指示处理数据 2. 确保数据安全 3. 记录处理活动 4. 在数据泄露时通知控制者 |
| **联合控制者** | 共同决定数据处理目的和方式的多个控制者 | 需明确责任分工并签署协议 |

**控制者与处理者的角色举例**

以下通过具体的案例说明数据控制者和数据处理者的角色划分及其责任。

**1. 电子商务平台案例**

**背景**

某电子商务平台（如亚马逊）处理用户的订单数据，包括姓名、地址、电话、购买记录等。平台决定如何收集、存储和使用这些数据，同时将支付处理交给第三方支付公司。

**角色划分**

* **控制者（Controller）**：电子商务平台
  + 决定用户数据的收集目的（如完成订单、营销）。
  + 决定数据处理的方式（如存储在自己的数据库中）。
  + 对用户数据的安全和合规负责。
* **处理者（Processor）**：第三方支付公司
  + 根据平台的指示处理用户的支付信息。
  + 不能将数据用于其他目的，例如分析用户行为，除非获得控制者的授权。

**责任**

* **控制者的责任**：确保支付公司有适当的数据安全措施，签订数据处理协议，通知用户其数据将用于支付处理。
* **处理者的责任**：严格按照合同条款处理数据，不能将支付数据用于其他目的，并在发生数据泄露时及时通知平台。

**2. 云存储服务案例**

**背景**

一家创业公司（如某健康应用）为用户提供健康记录管理服务，收集用户的健康数据（如血压、体重）。这家公司将所有用户数据存储在亚马逊AWS云服务上。

**角色划分**

* **控制者（Controller）**：健康应用公司
  + 决定收集哪些健康数据，以及如何处理这些数据（如生成健康报告）。
  + 负责数据的合规性及用户隐私保护。
* **处理者（Processor）**：亚马逊AWS
  + 为健康应用公司存储用户数据。
  + 不会对数据内容作出决定，仅根据健康应用公司的指示管理数据存储和访问权限。

**责任**

* **控制者的责任**：
  + 确保存储的数据仅用于合法目的，并采取必要的技术和组织措施保护数据安全。
  + 与AWS签订处理协议，明确数据存储要求和安全责任。
  + 若发生数据泄露，需在72小时内通知监督机构。
* **处理者的责任**：
  + 确保数据存储安全，防止未经授权的访问。
  + 若存储系统被黑客攻击，需立即通知健康应用公司。

**3. 市场营销案例**

**背景**

一家在线零售商决定进行电子邮件营销活动，向潜在客户发送广告邮件，并将这一任务外包给邮件营销服务提供商（如Mailchimp）。

**角色划分**

* **控制者（Controller）**：在线零售商
  + 决定收集客户的电子邮件地址及如何使用这些数据（如发送促销邮件）。
* **处理者（Processor）**：邮件营销服务提供商
  + 根据零售商提供的客户数据发送电子邮件。

**责任**

* **控制者的责任**：
  + 确保客户同意接收促销邮件（合法性）。
  + 与Mailchimp签订数据处理协议，明确双方的责任。
  + 若客户请求删除数据，需指示Mailchimp删除相关记录。
* **处理者的责任**：
  + 仅用于发送零售商指定的电子邮件，不得保存客户的电子邮件地址用于其他目的。
  + 确保其邮件系统的安全性，防止数据泄露。

**4. 联合控制者案例**

**背景**

两家公司共同开发了一款社交媒体应用（如图片分享平台），并共同决定用户数据的处理目的和方式，包括收集用户的照片、地理位置和好友列表。

**角色划分**

* **联合控制者（Joint Controllers）**：两家公司
  + 共同决定如何收集用户数据、用于哪些功能（如推荐好友）。
  + 需要签订协议，明确双方在数据处理中的具体责任。

**责任**

* **联合控制者的共同责任**：
  + 确保数据处理活动符合 GDPR 要求。
  + 向用户提供透明的信息，说明数据收集的目的和使用方式。
  + 若用户要求删除其数据，需双方协作完成。

**总结**

* **控制者**：负责数据处理的总体方向和目的，承担主要责任（如确保合法性、通知数据泄露）。
* **处理者**：按照控制者的指示处理数据，负责数据的具体操作和安全保障。
* **联合控制者**：共同决定数据处理的目的和方式，需明确责任分工并保持透明。