



20XX

专业合同封面

COUNTRACT COVER

甲方：XXX

乙方：XXX

P E R S O N A L

2025 年度电子商务平台数据安全保护合同标准范本

本合同目录一览

1. 定义与解释

1.1 合同术语定义

1.2 法律与法规适用

1.3 术语解释

2. 合同主体

2.1 合同双方基本信息

2.2 合同双方权利义务

2.3 合同主体变更

3. 数据安全保护目标

3.1 数据安全保护原则

3.2 数据安全保护目标

3.3 数据安全保护措施

4. 数据安全风险评估

4.1 风险评估方法

4.2 风险评估内容

4.3 风险评估结果与应用

5. 数据安全管理制度

5.1 数据安全管理制度概述

5.2 数据分类与分级

5.3 数据访问控制

5.4 数据备份与恢复

5.5 数据安全事件处理

6. 数据安全培训与宣传

6.1 培训内容与方式

6.2 宣传方式与范围

6.3 培训与宣传效果评估

7. 数据安全事件报告与处理

7.1 事件报告程序

7.2 事件处理流程

7.3 事件处理结果

8. 数据安全监督与检查

8.1 监督检查方式

8.2 监督检查内容

8.3 监督检查结果与应用

9. 违约责任与争议解决

9.1 违约责任

9.2 争议解决方式

9.3 争议解决程序

10. 合同期限与终止

10.1 合同期限

10.2 合同终止条件

10.3 合同终止程序

11. 合同变更与解除

11.1 合同变更

11.2 合同解除

11.3 合同变更与解除的效力

12. 合同附件

12.1 附件一：数据安全管理制度

12.2 附件二：数据安全事件报告表

12.3 附件三：其他相关文件

13. 合同生效与解除

13.1 合同生效条件

13.2 合同解除条件

13.3 合同生效与解除的程序

14. 其他约定

14.1 通知与送达

14.2 合同语言

14.3 合同解释与适用

14.4 合同附件效力

14.5 合同未尽事宜

第一部分：合同如下：

1. 定义与解释

1.1 合同术语定义

1.1.1 “电子商务平台”指通过互联网提供商品或服务交易的在线平台。

1.1.2 “数据”指电子商务平台收集、存储、使用和传输的各类信息，包括个人信息、交易信息、用户行为数据等。

1.1.3

“数据安全”指防止数据未经授权的访问、泄露、篡改、破坏和丢失。

1.1.4 “数据安全事件”指因黑客攻击、系统故障、人为错误等原因导致的数据安全事件。

1.2 法律与法规适用

本合同适用中华人民共和国法律、法规及相关政策，包括但不限于《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》等。

1.3 术语解释

本合同中未定义的术语，其含义应按照相关法律法规、国家标准或行业惯例进行解释。

2. 合同主体

2.1 合同双方基本信息

2.1.1 甲方（电子商务平台）：[甲方全称]，住所地：[甲方住所地]，法定代表人：[甲方法定代表人姓名]，联系电话：[甲方联系电话]。

2.1.2 乙方（数据安全服务商）：[乙方全称]，住所地：[乙方住所地]，法定代表人：[乙方法定代表人姓名]，联系电话：[乙方联系电话]。

2.2 合同双方权利义务

2.2.1 甲方有权要求乙方提供数据安全保护服务,并支付相应费用。

2.2.2 乙方应按照合同约定,履行数据安全保护职责,确保甲方数据安全。

2.3 合同主体变更

2.3.1 合同主体变更需提前 30 日书面通知对方,并经双方同意。

3. 数据安全保护目标

3.1 数据安全保护原则

3.1.1 遵循最小化原则,仅收集、存储和使用必要的数据库。

3.1.2 遵循安全性原则,采取必要措施保护数据库安全。

3.1.3 遵循合法性原则,依法收集、使用和传输数据。

3.2 数据安全保护目标

3.2.1 确保甲方数据不被未经授权的访问、泄露、篡改、破坏和丢失。

3.2.2 在发生数据安全事件时,及时采取措施减少损失,并向甲方报告。

3.3 数据安全保护措施

3.3.1 采取技术手段,如防火墙、入侵检测系统等,保护数据库安全。

3.3.2

制定数据安全管理制度，包括数据访问控制、数据备份与恢复等。

4. 数据安全风险评估

4.1 风险评估方法

4.1.1 采用定性分析与定量分析相结合的方法进行风险评估。

4.1.2 定期对数据安全风险进行评估，至少每年一次。

4.2 风险评估内容

4.2.1 数据安全风险识别与分析。

4.2.2 数据安全风险等级划分。

4.3 风险评估结果与应用

4.3.1 根据风险评估结果，制定相应的数据安全保护措施。

4.3.2 对高风险数据采取特殊保护措施。

5. 数据安全管理制度

5.1 数据安全管理制度概述

5.1.1 制定数据安全管理制度，明确数据安全保护的责任和义务。

5.1.2 对数据安全管理制度进行定期审查和更新。

5.2 数据分类与分级

5.2.1 对数据进行分类和分级，制定相应的保护措施。

5.3 数据访问控制

5.3.1 限制对数据的访问权限，确保数据安全。

5.3.2 对访问数据进行记录和审计。

5.4 数据备份与恢复

5.4.1 定期对数据进行备份，确保数据可恢复。

5.4.2 制定数据恢复计划，确保在数据丢失后能及时恢复。

5.5 数据安全事件处理

5.5.1 制定数据安全事件处理流程，包括报告、调查、处理和恢复等环节。

5.5.2 在发生数据安全事件时，及时采取措施减少损失，并向甲方报告。

8. 数据安全培训与宣传

8.1 培训内容与方式

8.1.1 乙方应定期对甲方员工进行数据安全培训。

8.1.2 培训内容包括数据安全意识、安全操作规范、应急响应流程等。

8.1.3 培训方式包括线上课程、线下讲座、案例分析等。

8.2 宣传方式与范围

8.2.1 乙方应在电子商务平台上设立数据安全宣传栏目。

8.2.2 通过邮件、短信等方式向用户推送数据安全知识。

8.3 培训与宣传效果评估

8.3.1 定期对培训效果进行评估，包括员工参与度、知识掌握程度等。

8.3.2 根据评估结果调整培训与宣传内容。

9. 数据安全事件报告与处理

9.1 事件报告程序

9.1.1 发生数据安全事件时，乙方应在 24 小时内向甲方报告。

9.1.2 报告内容包括事件概述、影响范围、初步分析等。

9.2 事件处理流程

9.2.1 乙方应根据事件性质和影响程度，启动相应应急响应措施。

9.2.2 事件处理过程中，乙方应与甲方保持沟通，及时更新事件进展。

9.3 事件处理结果

9.3.1 事件处理后，乙方应向甲方提交事件处理报告，包括处理过程、结果和后续改进措施。

10. 数据安全监督与检查

10.1 监督检查方式

10.1.1 甲方有权对乙方数据安全保护工作进行监督检查。

10.1.2 监督检查方式包括现场检查、远程监控、技术检测等。

10.2 监督检查内容

10.2.1 数据安全管理制度执行情况。

10.2.2 数据安全保护措施落实情况。

10.3 监督检查结果与应用

10.3.1 甲方应将监督检查结果反馈给乙方。

10.3.2 乙方应根据监督检查结果，及时改进数据安全保护工作。

11. 违约责任与争议解决

11.1 违约责任

11.1.1 任何一方违反合同约定，应承担相应的违约责任。

11.1.2 违约责任包括但不限于赔偿损失、支付违约金等。

11.2 争议解决方式

11.2.1 双方发生争议，应友好协商解决。

11.2.2 协商不成的，可提交仲裁委员会仲裁或依法向人民法院提起诉讼。

12. 合同期限与终止

12.1 合同期限

12.1.1 本合同自双方签字盖章之日起生效，有效期为一年。

12.2 合同终止条件

12.2.1 合同期满，双方无续签意愿的，合同自动终止。

12.2.2 发生合同约定的解除条件时，合同终止。

12.3 合同终止程序

12.3.1 合同终止前，双方应完成现有业务的交接工作。

12.3.2 合同终止后，双方应相互提供必要协助，确保合同终止后的合法权益。

13. 合同附件

13.1 附件一：数据安全管理制度

13.2 附件二：数据安全事件报告表

13.3 附件三：其他相关文件

14. 其他约定

14.1 通知与送达

14.1.1 任何一方发出的通知，应以书面形式发送至对方指定的地址。

14.1.2 通知自发送之日起视为送达。

14.2 合同语言

14.2.1 本合同以中文书写，具有同等法律效力。

14.3 合同解释与适用

14.3.1 本合同未尽事宜，按照相关法律法规、国家标准或行业惯例执行。

14.4 合同附件效力

14.4.1 本合同附件与本合同具有同等法律效力。

14.5 合同未尽事宜

14.5.1 本合同未尽事宜，由双方协商解决。

第二部分：第三方介入后的修正

15. 第三方介入

15.1 第三方概念

15.1.1 “第三方”指除甲方和乙方之外的独立主体，包括但不限于审计机构、认证机构、技术支持服务提供商、法律顾问等。

15.1.2 第三方介入是指在合同履行过程中，经甲乙双方同意，由第三方提供专业服务或协助。

15.2 第三方介入的同意

15.2.1 甲乙双方同意，在合同履行过程中，可引入第三方介入，但需书面通知对方，并经对方同意。

15.2.2 第三方介入的同意需在合同附件中明确。

15.3 第三方的责任与义务

15.3.1 第三方应具备相应的资质和能力,确保其提供的服务符合合同要求。

15.3.2 第三方应遵守保密义务,不得泄露甲乙双方的商业秘密和敏感信息。

15.3.3 第三方应按照合同约定,履行其职责,并对自己的工作成果负责。

15.4 第三方的权利

15.4.1 第三方有权根据合同约定,获得相应的报酬和费用。

15.4.2 第三方有权在合同约定的范围内,代表甲方或乙方进行必要的工作。

15.5 第三方与其他各方的划分

15.5.1 第三方与甲方、乙方之间的关系为委托关系,第三方对甲方或乙方的责任限于其提供的专业服务范围。

15.5.2 第三方不得超越其职责范围,对甲方或乙方的其他行为承担责任。

15.5.3 第三方在执行任务过程中,应遵守国家法律法规和行业规范。

16. 第三方责任限额

16.1 第三方的责任限额

16.1.1 第三方的责任限额由甲乙双方在合同中约定,并在合同附件中明确。

16.1.2 责任限额应根据第三方的资质、服务内容、风险程度等因素确定。

16.2 超额责任

16.2.1 如第三方在履行合同过程中造成甲方或乙方的损失,超出责任限额的部分,由第三方自行承担。

16.2.2 如第三方因故意或重大过失造成甲方或乙方的损失,无论是否超出责任限额,第三方均应承担全部责任。

17. 第三方介入的合同变更

17.1 合同变更

17.1.1 第三方介入导致合同内容变更的,甲乙双方应协商一致,并在合同附件中修改相关条款。

17.1.2 合同变更不影响合同其他条款的效力。

18. 第三方介入的争议解决

18.1 争议解决

18.1.1 第三方介入引起的争议,由甲乙双方协商解决。

18.1.2 协商不成的,可提交仲裁委员会仲裁或依法向人民法院提起诉讼。

19. 第三方介入的合同解除

19.1 合同解除

19.1.1 第三方介入不符合合同约定或法律法规要求的,甲乙双方有权解除合同。

19.1.2 合同解除后,第三方应退还已收取的报酬和费用。

20. 第三方介入的合同终止

20.1 合同终止

20.1.1 第三方介入的合同在合同期限届满或合同解除后终止。

20.1.2 合同终止后,第三方应向甲乙双方提供完整的工作报告和成果。

21. 第三方介入的后续事宜

21.1 后续事宜

21.1.1 第三方介入结束后,甲乙双方应按照合同约定,处理后续事宜,包括但不限于数据交接、服务延续等。

21.1.2 第三方应协助甲乙双方完成后续事宜的处理。

第三部分: 其他补充性说明和解释

说明一：附件列表：

1. 附件一：数据安全管理制度

要求：详细列出数据安全制度的内容，包括数据分类、访问控制、备份恢复、安全事件处理等。

说明：该附件是合同执行过程中的重要依据，确保数据安全保护措施得到有效实施。

2. 附件二：数据安全事件报告表

要求：制定标准化的数据安全事件报告表，包括事件概述、影响范围、处理措施等。

说明：该附件用于记录和报告数据安全事件，便于甲乙双方及时处理和评估风险。

3. 附件三：第三方资质证明文件

要求：提供第三方介入的资质证明文件，如营业执照、专业资格证书等。

说明：该附件用于验证第三方的资质和能力，确保其能够胜任合同约定的服务。

4. 附件四：第三方责任限额协议

要求：明确第三方的责任限额，包括赔偿金额、赔偿范围等。

说明：该附件用于保护甲乙双方的利益，确保第三方在违约情况下承担相应的责任。

5. 附件五：合同变更协议

要求：详细记录合同变更的内容，包括变更原因、变更条款、变更生效日期等。

说明：该附件用于记录合同变更的历史和具体内容，确保合同的有效性。

6. 附件六：争议解决协议

要求：明确争议解决的方式，包括协商、仲裁、诉讼等。

说明：该附件用于解决合同执行过程中可能出现的争议，确保双方的合法权益。

说明二：违约行为及责任认定：

1. 违约行为：

甲方违约行为：

未按时支付服务费用。

提供的数据不真实、不准确。

未按照合同约定提供数据安全保护服务。

乙方违约行为：

未按时完成数据安全保护工作。

提供的服务不符合合同约定。

未按照合同约定提供数据安全事件报告。

2. 责任认定标准：

甲方违约责任认定：

甲方未按时支付服务费用，应支付违约金。

甲方提供的数据不真实、不准确，导致乙方损失，甲方应赔偿乙方损失。

甲方未按照合同约定提供数据安全保护服务，乙方有权要求甲方承担违约责任。

乙方违约责任认定：

乙方未按时完成数据安全保护工作，应支付违约金。

乙方提供的服务不符合合同约定，导致甲方损失，乙方应赔偿甲方损失。

乙方未按照合同约定提供数据安全事件报告，甲方有权要求乙方承担违约责任。

3. 违约示例说明：

甲方未按时支付服务费用，乙方有权要求甲方支付违约金，违约金金额为应付款项的 5%。

甲方提供的数据不真实，导致乙方在风险评估过程中产生误判，乙方有权要求甲方赔偿因此产生的损失。

全文完。

2025 年度电子商务平台数据安全保护合同标准范本 1

合同目录

第一章 合同概述

1.1 合同背景

1.2 合同目的

1.3 合同范围

1.4 合同期限

1.5 合同双方

第二章 数据安全保护原则

2.1 依法合规原则

2.2 安全责任原则

2.3 保密原则

2.4 透明原则

2.5 完善原则

第三章 数据安全保护范围

3.1 数据类型

3.2 数据处理

3.3 数据存储

3.4 数据传输

3.5 数据销毁

第四章 数据安全保护措施

4.1 技术措施

4.2 管理措施

4.3 人员措施

4.4 应急措施

4.5 监测措施

4.6 风险评估

第五章 数据安全事件处理

5.1 事件报告

5.2 事件调查

5.3 事件应对

5.5 事件通报

第六章 数据安全责任

6.1 数据安全责任主体

6.2 数据安全责任划分

6.3 违约责任

6.4 责任追究

第七章 合同履行与监督

7.1 合同履行

7.2 监督机制

7.3 监督内容

7.4 监督方式

7.5 监督结果

第八章 合同变更与解除

8.1 合同变更

8.2 合同解除

8.3 合同终止

8.4 合同续签

第九章 合同争议解决

9.1 争议解决方式

9.2 争议解决机构

9.3 争议解决程序

9.4 争议解决费用

第十章 合同生效与终止

10.1 合同生效

10.2 合同终止

10.3 合同解除

10.4 合同续签

第十一章 违约责任

11.1 违约情形

11.2 违约责任

11.3 违约赔偿

11.4 违约处理

第十二章 合同附件

12.1 附件一：数据安全保护方案

12.2 附件二：数据安全事件应急预案

12.3 附件三：数据安全责任书

12.4 附件四：其他相关文件

第十三章 合同签署与备案

13.1 合同签署

13.2 合同备案

13.3 合同生效

13.4 合同变更

第十四章 合同其他事项

14.1 合同解释

14.2 合同语言

14.3 合同适用法律

14.4 合同附件

14.5 合同签署日期

合同编号_____

第一章 合同概述

1.1 合同背景

1.1.1 本合同背景基于《中华人民共和国网络安全法》、《中华人民共和国数据安全法》等相关法律法规，以及电子商务平台数据安全保护的
实际需求。

1.1.2 本合同旨在明确电子商务平台数据安全保护的责任和义务，确保数据安全，维护用户合法权益。

1.2 合同目的

1.2.1 明确电子商务平台数据安全保护的责任主体。

1.2.2 规范电子商务平台数据安全保护措施。

1.2.3 确保电子商务平台数据安全，防止数据泄露、篡改、破坏等安全事件发生。

1.3 合同范围

1.3.1 本合同适用于电子商务平台所有涉及数据安全保护的业务活动。

1.3.2 本合同不适用于第三方服务提供商的数据安全保护。

1.4 合同期限

1.4.1 本合同自双方签字盖章之日起生效，有效期为一年。

1.4.2 合同期满前一个月，双方可协商续签本合同。

1.5 合同双方

1.5.1 甲方：电子商务平台运营方

1.5.2 乙方：数据安全服务提供商

第二章 数据安全保护原则

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如
要下载或阅读全文，请访问：

<https://d.book118.com/988074003075007030>