20XX

# 专业合同封面

COUNTRACT COVER

甲 方： XXX

乙 方： XXX

PERSONAL

# 2024版食品行业数据安全保护合同范本

**本合同目录一览**

10.1 争议解决方式

10.2 争议解决程序

11. 法律适用

11.1 合同适用法律

11.2 适用法律解释

12. 合同生效

12.1 合同生效条件

12.2 合同生效日期

13. 合同附件

13.1 附件一：数据安全保护措施

13.2 附件二：数据安全事件应急处理预案

14. 其他约定事项

**第一部分：合同如下：**

1. 合同双方基本信息

1.1 合同双方名称

甲方：[甲方全称]

乙方：[乙方全称]

1.2 合同双方地址

甲方地址：[甲方详细地址]

乙方地址：[乙方详细地址]

1.3 合同双方联系方式

甲方联系方式：[甲方联系人姓名、电话、邮箱]

乙方联系方式：[乙方联系人姓名、电话、邮箱]

2. 合同背景及目的

2.1 合同签订背景

鉴于甲方从事食品行业，乙方具备数据安全保护相关技术和服务能力，双方经友好协商，达成共识，签订本合同。

2.2 合同签订目的

本合同旨在明确双方在食品行业数据安全保护方面的权利、义务和责任，确保数据安全，保护双方合法权益。

3. 数据安全保护原则

3.1 数据安全保护的基本原则

（1）合法、合规原则：双方在数据处理过程中，遵守国家相关法律法规，确保数据处理合法合规。

（2）安全、保密原则：采取必要的技术和管理措施，确保数据安全，防止数据泄露、篡改和破坏。

（3）最小化原则：仅收集、存储和使用为实现合同目的所必需的数据。

3.2 数据安全保护的具体要求

（1）数据分类：根据数据敏感程度，对数据进行分类管理。

（2）访问控制：建立严格的访问控制机制，限制对数据的访问权限。

（3）数据加密：对传输和存储的数据进行加密处理，防止数据泄露。

（4）数据备份：定期对数据进行备份，确保数据可恢复。

4. 数据安全责任划分

4.1 数据安全责任主体

甲方负责确保数据安全，包括但不限于数据的收集、存储、处理、传输和销毁等环节。

乙方负责提供数据安全保护相关技术和服务，协助甲方实现数据安全保护。

4.2 数据安全责任范围

（1）甲方责任：

1.1.1 按照国家相关法律法规和本合同约定，负责数据安全保护；

1.1.2 提供必要的技术支持，确保数据安全；

1.1.3 对乙方提供的数据安全保护技术和服务进行监督和评估。

（2）乙方责任：

1.2.1 按照国家相关法律法规和本合同约定，提供数据安全保护技术和服务；

1.2.2 对甲方提供的数据进行安全处理，确保数据安全；

1.2.3 对数据安全事件进行应急处理，及时报告甲方。

5. 数据安全保护措施

5.1 数据收集与存储安全

（1）数据收集：甲方在收集数据时，应遵循最小化原则，仅收集为实现合同目的所必需的数据。

（2）数据存储：乙方采用安全可靠的存储设备和技术，确保数据存储安全。

5.2 数据传输安全

（1）数据传输：乙方采用加密技术，确保数据在传输过程中的安全。

（2）传输渠道：使用安全的传输渠道，如专线、VPN 等。

5.3 数据处理安全

（1）数据处理：乙方在数据处理过程中，遵循数据安全保护原则，确保数据处理安全。

（2）数据处理权限：对数据处理权限进行严格控制，防止数据被非法使用。

5.4 数据共享与开放安全

（1）数据共享：在共享数据前，确保数据安全，防止数据泄露。

（2）数据开放：在开放数据前，对数据进行脱敏处理，确保数据安全。

5.5 数据安全事件应急处理

（1）事件报告：发现数据安全事件时，乙方应立即向甲方报告。

（2）事件调查：乙方配合甲方进行调查，找出事件原因。

（3）事件处理：乙方采取必要措施，防止事件扩大，并协助甲方恢复正常运营。

8. 合同履行期限及终止

8.1 合同履行期限

本合同自双方签字盖章之日起生效，合同期限为[具体期限]，自合同生效之日起计算。

8.2 合同终止条件

（1）合同期限届满，双方无续签意向；

（2）任何一方违反合同约定，经另一方书面通知后，未在[具体期限]内纠正；

（3）发生不可抗力事件，导致合同无法履行；

（4）双方协商一致，决定终止合同。

9. 违约责任

9.1 违约情形

（1）任何一方未按照合同约定履行数据安全保护义务；

（2）任何一方泄露、篡改、破坏数据；

（3）任何一方未按照合同约定提供数据安全保护技术和服务；

（4）任何一方未按照合同约定进行数据安全事件报告和处理。

9.2 违约责任承担

（1）违约方应承担由此给对方造成的损失；

（2）违约方应按照合同约定支付违约金；

（3）违约方应承担由此引起的法律责任。

10. 争议解决

10.1 争议解决方式

双方发生争议，应通过友好协商解决；协商不成的，提交[具体仲裁机构或法院]仲裁或诉讼。

10.2 争议解决程序

（1）争议发生后，双方应在[具体期限]内提出书面争议解决请求；

（2）争议解决过程中，双方应继续履行合同义务；

（3）仲裁或诉讼过程中，双方应积极配合，提供必要的证据和资料。

11. 法律适用

11.1 合同适用法律

本合同适用中华人民共和国法律。

11.2 适用法律解释

本合同条款的解释，以中华人民共和国法律为准。

12. 合同生效

12.1 合同生效条件

本合同经双方签字盖章后生效。

12.2 合同生效日期

本合同自双方签字盖章之日起生效。

13. 合同附件

## 13.1 附件一：数据安全保护措施

详细列明双方在数据安全保护方面的具体措施。

13.2 附件二：数据安全事件应急处理预案

详细说明数据安全事件发生时的应急处理流程和措施。

14. 其他约定事项

14.1 本合同未尽事宜，由双方另行协商解决。

14.2 本合同一式两份，双方各执一份，具有同等法律效力。

14.3 本合同自双方签字盖章之日起生效，自合同终止之日起失效。

**第二部分：第三方介入后的修正**

15. 第三方介入的定义与范围

15.1 第三方定义

在本合同中，“第三方”是指除甲方、乙方以外的任何个人、法人或其他组织，包括但不限于中介方、咨询方、技术服务提供方、监管机构等。

15.2 第三方介入范围

（1）提供数据安全保护相关的技术、咨询或服务；

（2）协助双方进行数据安全评估和监督；

（3）处理数据安全事件；

（4）进行合同履行的监督和协调。

16. 第三方介入的程序

16.1 介入申请

（1）甲方或乙方如需第三方介入，应向对方提出书面申请，并说明介入的原因、目的和预期效果。

（2）对方应在[具体期限]内回复是否同意第三方介入。

16.2 介入协议

（1）双方同意第三方介入后，应与第三方签订单独的协议，明确各方的权利、义务和责任。

（2）第三方介入协议应与本合同保持一致，不得与本合同相冲突。

17. 甲乙方责任与第三方责任划分

17.1 甲乙方责任

（1）甲方和乙方应确保第三方介入符合合同目的，并对其提供的数据和信息保密。

（2）甲方和乙方应向第三方提供必要的协助和便利，确保第三方能够有效履行其职责。

17.2 第三方责任

（1）第三方应按照合同约定和法律法规的要求，履行其职责，并对提供的服务或技术负责。

（2）第三方应遵守数据安全保护的相关规定，确保数据安全。

18. 第三方责任限额

18.1 责任限额定义

本合同中的“责任限额”是指第三方因履行合同义务或提供的服务导致甲方或乙方遭受损失时，第三方应承担的最高赔偿责任。

18.2 责任限额确定

（1）责任限额应根据第三方提供的服务或技术的重要性、潜在风险以及合同金额等因素综合确定。

（2）责任限额应在第三方介入协议中明确约定。

18.3 责任限额的适用

（1）责任限额仅适用于第三方因履行合同义务或提供的服务导致甲方或乙方遭受的直接经济损失。

（2）责任限额不适用于因第三方故意或重大过失导致的损失。

19. 第三方变更与退出

19.1 第三方变更

（1）如第三方需要变更，应提前[具体期限]通知甲方和乙方，并获得双方同意。

（2）第三方变更后，应与新第三方签订新的协议，并确保新第三方符合合同要求。

19.2 第三方退出

（1）如第三方退出，应提前[具体期限]通知甲方和乙方，并确保其职责的顺利交接。

（2）第三方退出后，甲方和乙方应重新评估数据安全保护的需求，并采取必要措施确保数据安全。

20. 第三方介入合同的终止

20.1 终止条件

（1）合同期限届满或提前终止；

（2）第三方完成其职责，或甲方和乙方决定不再需要第三方介入；

（3）第三方无法履行其职责，经甲方和乙方协商一致后终止。

20.2 终止程序

（2）甲方和乙方应在[具体期限]内确认第三方的工作成果，并对第三方进行评价。

（3）合同终止后，第三方应将所有与合同相关的文件、资料和设备移交给甲方或乙方。

**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：数据安全保护措施

详细要求：包括但不限于数据收集、存储、传输、处理、共享、开放等环节的具体安全措施。

说明：此附件为合同附件，甲方和乙方应共同遵守附件中规定的数据安全保护措施。

2. 附件二：数据安全事件应急处理预案

详细要求：包括数据安全事件报告、调查、处理、恢复等环节的应急处理流程和措施。

说明：此附件为合同附件，用于指导甲方和乙方在发生数据安全事件时的应急处理。

3. 附件三：第三方介入协议

详细要求：包括第三方介入的目的、范围、责任、权利、义务、期限、终止条件等内容。

说明：此附件为合同附件，用于规范第三方介入的行为和责任。

4. 附件四：数据安全评估报告

详细要求：包括数据安全风险评估的结果、发现的问题、改进建议等内容。

说明：此附件为合同附件，用于记录数据安全评估的结果。

5. 附件五：数据安全事件报告

详细要求：包括数据安全事件发生的时间、地点、原因、影响、处理结果等内容。

说明：此附件为合同附件，用于记录和报告数据安全事件。

6. 附件六：合同履行情况报告

详细要求：包括合同履行情况、存在的问题、改进措施等内容。

说明：此附件为合同附件，用于记录合同履行过程中的情况。

说明二：违约行为及责任认定：

1. 违约行为

未按照合同约定提供数据安全保护措施；

泄露、篡改、破坏数据；

未按照合同约定进行数据安全事件报告和处理；

未按照合同约定提供数据安全保护技术和服务；

未遵守数据安全保护的相关规定。

2. 责任认定标准

违约方应根据违约行为对另一方造成的实际损失承担赔偿责任；

违约方应按照合同约定支付违约金；

违约方应承担由此引起的法律责任。

3. 违约示例说明

甲方未按照合同约定提供数据安全保护措施，导致乙方数据泄露，甲方应承担由此给乙方造成的经济损失和法律责任；

乙方未按照合同约定进行数据安全事件报告，导致事件扩大，乙方应承担相应的违约责任；

第三方在提供数据安全保护服务时，由于自身原因导致数据安全事件，第三方应按照合同约定承担赔偿责任。

全文完。

# 2024 版食品行业数据安全保护合同范本 1

**本合同目录一览**

5.3 数据安全事件调查与处理

6. 数据安全监督检查

6.1 监督检查范围

6.2 监督检查方式

6.3 监督检查结果处理

7. 数据安全争议解决

7.1 争议解决方式

7.2 争议解决程序

7.3 争议解决费用

8. 合同生效、变更与解除

8.1 合同生效条件

8.2 合同变更程序

8.3 合同解除条件

8.4 合同解除程序

9. 合同终止后的数据处理

9.1 数据存储与备份

9.2 数据销毁

9.3 数据归档

**第一部分：合同如下：**

1. 合同基本信息

1.1 合同名称：本合同名称为“2024版食品行业数据安全保护合同”。

**1.2 合同编号：本合同编号为_____。**

1.3 合同签订日期：本合同签订日期为_____。

1.4 合同双方当事人信息：

1.4.1 甲方（数据控制方）：_____，住所地：_____，法定代表人：_____。

1.4.2 乙方（数据处理方）：_____，住所地：_____，法定代表人：_____。

2. 定义与解释

2.1 数据安全：指在数据生命周期内，确保数据不被未授权访问、篡改、泄露、破坏、丢失或滥用，以及防止数据被非法获取、泄露或损害。

2.2 数据泄露：指未经授权的第三方获取了数据，或者数据被非法泄露到公开渠道。

2.3 数据处理：指对数据进行收集、存储、使用、传输、删除等操作。

2.4 数据传输：指将数据从一个地点传输到另一个地点。

2.5 数据存储：指将数据存储在电子或物理介质上。

3. 数据安全保护措施

3.1 数据加密：乙方应采用行业标准的加密技术对甲方数据进行加密存储和传输。

3.2 访问控制：乙方应建立严格的访问控制机制，确保只有授权人员才能访问数据。

3.3 安全审计：乙方应定期进行安全审计，确保数据安全保护措施得到有效执行。

3.4 安全事件处理：乙方应制定安全事件处理流程，及时响应并处理数据安全事件。

3.5 数据备份与恢复：乙方应定期进行数据备份，并确保在数据丢失或损坏时能够及时恢复。

4. 数据安全责任与义务

4.1 数据安全保护责任：乙方应承担数据安全保护责任，确保甲方数据的安全。

4.2 数据安全保密义务：乙方应遵守保密义务，不得泄露甲方数据。

4.3 数据安全培训：乙方应对其员工进行数据安全培训，提高员工的数据安全意识。

4.4 数据安全评估：乙方应定期进行数据安全评估，评估结果应报甲方。