《个人信息委托处理协议》

单击或点击此处输入文字。

—作为委托方—

和

单击或点击此处输入文字。

—作为受托方—

版本号：2023 版

联系方式	
委托方	
公司名称	单击或点击此处输入文字。
地址	单击或点击此处输入文字。
联系人	单击或点击此处输入文字。
电话	单击或点击此处输入文字。
电子邮箱	单击或点击此处输入文字。
受托方	
公司名称	单击或点击此处输入文字。
地址	单击或点击此处输入文字。
联系人	单击或点击此处输入文字。
电话	单击或点击此处输入文字。
电子邮箱	单击或点击此处输入文字。

1. 适用

1.1 本《个人信息委托处理协议》（**“本协议”**）适用于受托方作为委托方的供应商或合作伙伴，在向委托方提供货物或服务的过程中，接受委托方的委托，代表委托方处理个人信息的相关活动。

1.2 本协议附件 1 数据处理问卷（**“附件 1”**）问卷 A 由委托方填写，受托方应提供一切必要的支持与协助，除非经委托方同意，受托方在履行本协议过程中开展的相关活动不得超出附件 1 问卷 A 约定的范围。本协议附件 1 问卷 B 由受托方填写，构成受托方于本协议项下的陈述与保证。受托方在履行本协议的过程中，如需对本协议附件 1 问卷 B 中信息进行更新和修改，其应及时告知委托方。

2. 定义

在本协议中：

2.1 **“数据保护法律和法规”**指适用于委托方或受托方的，有关个人信息安全、数据安全及网络安全的所有法律、法规和国家标准，包括且不限于《中华人民共和国个人信息保护法》、《中华人民共和国数据安全法》、《中华人民共和国网络安全法》等。

2.2 **“数据保护及信息安全措施”**指本协议附件 1 问卷 B 中所列的措施以及其他本协议所约定、或履行本协议所需的措施。

2.3 **“中国”**指中华人民共和国，出于本协议之目的，不包括香港特别行政区、澳门特别行政区和台湾地区。

2.4 **“处理”**指包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等活动。

2.5 **“个人信息”**指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

2.6 “**个人信息安全事件**”指个人信息出现未授权使用、未授权或意外修改、损毁或者泄露、篡改、丢失、擅自传输、擅自处理及其他形式的滥用。

2.7 “**书面**”指合同书、信件和数据电文（包括电报、电传、传真、电子数据交换和电子邮件）等可以有形地表现所载内容的形式。

3. 受托方处理权限

3.1 受托方在处理委托方提供的个人信息时，应遵守适用的数据保护法律和法规。

3.2 受托方在处理委托方提供的个人信息时，应仅严格遵照委托方的指示。除了双方在本协议附件 1 问卷 A 中做出的约定，所有指示必须由委托方以书面形式做出。

3.3 受托方不得超出上述指示，为了自身或第三方的目的，处理委托方向其提供的个人信息。如果受托方认为委托方给出的指示可能违反适用的数据保护法律和法规，或者因

其他特殊原因无法按照委托方的指示处理个人信息，届时，双方应积极沟通，就相关细节达成一致。

3.4 除非获得委托方事先书面同意或本协议另有约定，受托方不应将任何委托方提供的个人信息传输至任何第三方，且不得允许任何第三方获取该等个人信息。

3.5 除非双方另有书面约定，对于委托方向受托方提供的个人信息，受托方不享有自主决定相关处理活动的权利，且受托方不应由于履行本协议而取得可适用法律法规项下的对于该等信息副本或复制品的相应权利。

4. 受托方的义务

4.1 受托方应按照数据保护法律和法规，采取必要措施保障所处理的个人信息的安全，并协助委托方履行数据保护法律和法规的相关义务。

4.2 受托方应协助委托方响应个人信息主体的相应权利，包括但不限于要求知情、决定、查阅、复制、更正、补充、删除个人信息等权利。如果个人信息主体就上述权利与受托方直接联系，受托方应立即将该等请求书面转告至委托方，并根据委托方的指示处理：（1）若未获得委托方授权，受托方不得直接响应个人信息主体的行权请求；（2）若委托方授权受托方直接响应，受托方应在委托方授权范围内响应个人信息主体行权请求。

4.3 受托方应对参与处理委托方提供的个人信息的人员进行数据保护培训。

4.4 受托方应按照可适用的法律法规建立数据保护和个人信息保护的机制、系统和流程。

4.5 经委托方要求，受托方应提供合理且必要的信息和材料，协助委托方履行适用的数据保护法律和法规要求的各项义务，例如，可适用的法律法规要求的通知义务、记录处理活动、开展个人信息安全影响评估以及申报网络安全审查（如适用）等义务。

4.6 除非双方另有书面约定，受托方应承担其为履行本协议项下职责和义务相关的所有成本、费用或支出。

4.7 委托方可在合理的期间内，提前要求受托方归还委托处理的个人信息及其副本，和/或永久且安全地删除或销毁本协议项下处理的相关个人信息及其副本，如果个人信息已被删除，受托方需确保无法对个人信息进行复原。委托方有权合理要求受托方提供相关材料证明其已完成前述要求。

4.8 本协议项下有关个人信息的处理应仅限于在中国境内进行。未经委托方的事先书面同意或授权，受托方不得向境外提供任何本协议项下的有关个人信息，包括但不限于：（1）不得在中国以外访问或提供机会让他人访问有关个人信息；（2）不得使任何个人信息转移至中国以外的其他国家或地区；且（3）不应有数据保护法律和法规规定的其他数据出境行为。经委托方要求，受托方应在最大合理程度内配合委托方，以便遵守中国对数据出境的相关合规要求（包括但不限于完成个人信息保护影响评估、数据出境安

全评估、个人信息出境标准合同备案、个人信息保护认证等）。如受托方违反本第 4.8 条的任何规定，委托方有权立即终止本协议，且有权要求受托方根据本协议第 9 条承担违约责任。

4.9 如果任何第三方收购受托方多数股份或者表决权或者全部或实质性全部资产或业务，或者受托方的主营业务发生实质性变更，委托方有权终止本协议。届时，双方应就相关细节进行沟通。

4.10 受托方应促使其关联、附属机构及其各自分包商（如有）、员工、董事、监事、代理或管理人员等能够接触任何受托处理的个人信息的人士遵守本协议中受托方的义务，受托方应确保该等人士知悉并遵守严格程度不低于本协议义务的约束。

5. 分包商

5.1 对于受托方聘用分包商的，受托方必须事先获取委托方的书面同意。受托方与分包商之间的合同安排，必须符合本协议的约定和要求。尤其是，受托方必须确保委托方可根据本协议第 7 条对分包商进行核查。受托方应向委托方提供关于聘用分包商的所有信息，包括但不限于相关合同文件供委托方审查。

5.2 受托方应填写本协议附件 1 问卷 C 中的分包商信息。受托方应确保该类分包商能够采取与受托方相同的方式遵守本协议附件 1 问卷 B 中所列的数据保护及信息安全措施。

5.3 如果受托方有意在本协议期限内更换或增加分包商，并且在委托方同意的前提下，受托方应将本协议附件 1 问卷 C 的更新版本提供给委托方。

5.4 在履行本协议的过程中，受托方应就分包商在本协议项下的职责和义务向委托方承担相应责任。

6. 信息安全

6.1 受托方保证，其将通过与处理活动风险相适宜的数据保护及信息安全措施（包括且不限于附件 1 问卷 B 中所涉及的数据保护及信息安全措施）来处理委托方提供的个人信息，以防止发生个人信息安全事件。受托方应完整填写本协议附件 1 问卷 B 中的数据保护及信息安全措施。无论本协议是否到期或终止，以上措施应在受托方处理或者聘用分包商处理委托方提供之个人信息的期限内持续适用。如果委托方根据适用的数据保护法律和法规要求，认为受托方需采取额外的安全措施，则其可要求受托方实施该等额外措施。

6.2 受托方应建立信息安全管理体系、执行措施及风险应对措施。受托方应定期更新、修订该等体系及措施并相应记录。

6.3 应委托方要求，受托方应当将数据保护及信息安全措施的实施情况告知委托方。

6.4 如受托方已完成信息安全管理体系的认证，例如 ISO27001，应向委托方提供相应文件。

6.5 在履行本协议的过程中，受托方仅在履行本协议范围内，可向其人员和分包商授予相应的权限，并且仅可允许该类人员执行与履行本协议相关的任务。

6.6 如果本协议附件 1 问卷 B 描述的数据保护及信息安全措施出现重大变动，受托方必须以书面形式通知委托方。

7. 检查

7.1 委托方或者委托方代表有权对受托方是否满足本协议要求开展检查。受托方应提供所需信息。如果委托方得知或者发现受托方：（1）未按照指示或者本协议要求处理个人信息；或（2）受托方未能有效履行个人信息安全保护责任，受托方应按照委托方要求停止相关行为，配合委托方指示采取有效补救措施（例如更改口令、回收权限、断开网络连接等），或消除个人信息面临的安全风险。此外，经委托方要求，受托方应在合理时间内，将委托方提供的问卷调查填写完整并提交证明其满足相应义务的文件，或者以书面确认本协议附件 1 问卷 B 中的措施是适当且及时更新的。

7.2 在事先通知的情况下，委托方或者委托方代表可以获得访问受托方办公地点以及受托方处理委托方提供的个人信息的信息技术系统的授权，以便委托方对本协议的实施情况以及数据保护及信息安全措施的适用性进行验证。

7.3 如果监管部门对于受托方和/或受托方使用的信息技术基础设施及系统采取控制程序或其他强制措施，且该等措施与本协议有关或可能影响到本协议的履行，受托方应立即书面通知委托方。如因相关部门开展查封、扣押、司法调查或其他执法行为，或因破产程序、重组程序或者第三方开展的其他活动或者行动，阻碍本协议的履行，受托方应将该等情况立即书面通知委托方。

7.4 在第 7.3 条所规定的情形下，如果受托方接受与委托方提供的个人信息相关的检查、访问或者其他有关授权访问，受托方应采取充分措施确保个人信息的安全。

7.5 受托方同意，委托方可聘用独立第三方机构开展本第 7 条约定的各项检查活动。

8. 个人信息安全事件

8.1 如果有任何已发生的个人信息安全事件，受托方应尽快通知委托方（且任何情形下不应超出其知晓上述情形后 48 小时），以便委托方能够根据适用的数据保护法律和法规评估下一步计划。

8.2 根据委托方的要求，受托方应采取包括但不限于以下措施：（1）尽快采取必要措施澄清并补救个人信息安全事件，包括但不限于停止非法处理、恢复丢失或损坏的个人信息（如可行）、消除一切非法处理手段或措施已造成的影响、升级优化技术和组织安全措施等；（2）向委托方提供用以记录该事件并将视情况向有关监管机构报告、或通知个人信息主体所必要的信息和协助。

9. 违约责任

9.1 受托方不履行或不完全履行本协议任一条款（包括但不限于不履行或不完全履行本协议下的义务）或数据保护法律和法规，即构成违约（“**违约**”）。

9.2 受托方违约的情形下，委托方有权：

(1) 采取有效补救措施（如暂停传输个人信息、更改口令、回收权限、断开网络连接等）控制或消除因受托方的违约给委托方提供的个人信息带来的安全风险；

(2) 按照可适用的法律法规，追究受托方的违约责任，包括但不限于要求受托方赔偿委托方、其关联、附属机构及其各自分包商（如有）、员工、董事、监事、代理或管理人员（合称“**受偿方**”）造成的损失、费用和罚款（合称“**索赔**”，包括诉讼费用、可预见的合理利润或收入的损失，和/或个人信息主体或政府部门就个人信息处理而提出的申诉或主张等）；

(3) 要求受托方按照本协议的约定继续履行相关义务；以及

(4) 根据本协议第 10.1 条终止本协议。

9.3 若受托方违约，在不影响受偿方依据中国法律或与本协议有关的任何其他权利或救济的情况下，受托方应按照可适用的法律法规：

(1) 为受偿方辩护并使其免于遭受因受托方的任何违约引起或与之相关的给受偿方造成的索赔，并就该等索赔向受偿方做出相应赔偿；以及

(2) 协助受偿方对索赔进行抗辩，始终根据受偿方的指示行事，使受偿方免受损害，并自行承担因此而产生的其他损失或法律责任。

10. 通用条款

10.1 本协议自[请输入生效日 xx 年 xx 月 xx 日]起生效，本协议有效期限截至[请输入截止日期（与商业合同一致）xx 年 xx 月 xx 日]为止。如受托方违约，在不影响委托方基于法律法规和本协议赋予的权利和救济的情况下，委托方可随时书面通知受托方终止本协议且不承担违约责任。

10.2 本协议期限届满或终止之日，受托方应根据委托方的要求，立即向委托方归还所有委托处理的个人信息及其副本，和/或永久且安全地删除或销毁所有委托处理的个人信息及其副本。如果个人信息已被删除，受托方需确保无法对个人信息进行复原。委托方有权合理要求受托方提供相关材料证明其已完成前述要求。

10.3 对本协议及其任何部分的变更、补充或修订均需双方的书面同意。

10.4 本协议的签署、解释和履行以及由本协议引起或与之相关的任何争议应受中国法律管辖。

10.5 若本协议的任何条款被认定为无效或不可执行，此等条款的无效性将不影响本协议的其他条款，且所有未受此无效性影响的条款仍具有完整效力和作用。

10.6 本协议附件应被视为本协议的组成部分，与本协议正文具有同等效力。

10.7 本协议一式两份，委托方与受托方各执一份，每份均为正本且具有同等法律效力。

签字及盖章

委托方： 单击或点击此处输入文字。 **（盖章）**

姓名：单击或点击此处输入文字。 **姓名：**单击或点击此处输入文字。

职务：单击或点击此处输入文字。 **职务：**单击或点击此处输入文字。

签字： **签字：**

日期： **日期：**

地点： **地点：**

受托方：单击或点击此处输入文字。 **（盖章）**

姓名：单击或点击此处输入文字。

职务：单击或点击此处输入文字。

签字：

日期：

地点：

附件 1：数据处理问卷

本附件为《个人信息委托处理协议》的组成部分。由**问卷 A. 委托处理基本情况**，**问卷 B. 数据保护及信息安全措施**，**问卷 C. 批准分包商（如适用）**组成。

问卷 A. 委托处理基本情况

1 主要事项

请详细描述是否存在与上述委托处理相关的主协议或其他（服务）协议（“相关协议”）以及受托方提供的服务。如：受托方与委托方签署 XXX 协议，提供 XXX 货物 / 服务，通过 XXX 涉及和 / 或处理个人信息。

2 委托处理期限

一般情况下，委托处理期限与本协议第 10.1 条规定的协议期限一致。若委托处理期限与本协议第 10.1 条规定协议期限不一致，请具体说明委托处理期限。

3 所处理个人信息的类型

列举个人信息的类型（其中，个人敏感信息类型**加粗并下划线**），示例：姓名，地址，电话，用户 ID，车辆数据（请明确具体类型），**信用卡数据**，**身份证号**，**身份证扫描件**，**驾驶证号**，**驾驶证扫描件**等。

4 数据处理和保存地点

请列举所有个人信息将被处理及保存的地点，如：数据中心或者办公室，以及所有基于测试和运维目的（远程）访问个人信息的地址，请明确上述地点的城市。

5 可能开展的个人信息处理活动和目的

受托方应针对第 3 子条款中规定的个人信息类型为委托方提供下列服务：

请具体描述受托方就委托方提供的个人信息进行的处理操作，处理个人信息基本意味着所有与个人信息相关的动作，例如收集、存储、使用、加工、传输、提供、公开、删除等。如该等动作已经涵盖在相关协议中，可以采取以下引用相关协议描述的方式：例如，“受托方根据相关协议 XXX 条，提供关于问卷 A 第 3 款涉及的个人信息的 XXX 服务”。

6 所涉及的个人信息主体

在本协议范围内，委托处理的个人信息所标识或者关联的自然人（个人信息主体）如下所示：

请具体描述本服务中委托处理的个人信息所标识或者关联的自然人类型，例如，某公司的雇员，XXX 服务的客户，XXX 应用的用户，司机，供应商等。若主协议已涵盖该类描述，需要体现对于主协议的引用：例如，“相关协议/附件第 XXX 条已规定服务涉及的人员”。若涉及不满 14 周岁未成年人的个人信息，请列明并描述原因。

问卷 B. 数据保护及信息安全措施

受托方**已采取下述基本措施及补充措施（如适用）**，以保障数据及信息安全。(填入“是”标识已采取的措施，填入“否”标识未采取的措施，并在方框内根据需要补充描述)。

本部分用于记录由受托方实施的数据保护及信息安全措施，以保障数据处理活动的安全性。

每项数据保护及信息安全措施根据其主要保护目标进行分类：处理个人信息所涉及的系统和服务的机密性，完整性，可用性和韧性（可复原性)。组织措施及与流程有关的措施是对主要保护目标的补充。

下面列出的所有领域措施中的基本措施是必须采取的，如果未采取某项基本措施，请分别说明原因或替代措施。受托方需要确保根据现有技术采取了适当保护的水平。现有技术包括目前市场上可用的有效措施；国家或国际标准等提供了更具体的规范（例如 ISO27000, ISO27701, BSI, ENISA，NIST，TeleTrust 等)。

1 机密性-物理保护机密性

1.1 基本措施

序号	基本措施	是否已采取该措施（请填入“是”或“否”）	基本措施是必须采取的，如果未采取基本措施，请说明您的原因或替代措施
1	具有访问授权的人员的定义和文档，包括权限范围		单击或点击此处输入文字。
2	制定外部访客的出入规则(如陪同、出入禁令、身份证)		单击或点击此处输入文字。
3	以外部围墙的形式提供出入保护		单击或点击此处输入文字。
4	执行管理密钥使用的规则(包括安全锁定系统)		单击或点击此处输入文字。

（如需要，请在此补充）

1.2 补充措施

除《个人信息委托处理协议》中的基本要求外，为实施物理访问控制还采取了以下哪些行动？

序号	补充措施	是否已采取该措施（请填入“是”或“否”）
1	所有进出人员都有记录，门禁进出记录可查	
2	采取有室外安全措施的保障(如出入障碍设置、视频监控和探测传感器)	
3	访问授权 id 是分布式的	

4	要求员工身份证或在公司场所和建筑物公开携带员工身份证	
5	工作时间的大门和接待人员	
6	在工作时间以外为物业提供保安服务	
7	入口有身份识别器保护	
8	一楼/地下室有防盗窗	
9	设备安全，防止盗窃，物理操作和损坏	
10	建立不同的安全区域(例如访客会议室、工作站、服务器室、开发)	
11	更高安全级别：监控设备(如报警系统、视频监控)	
12	分离装置	
13	把工作用的电脑锁在房间里	
14	装有服务器的房间都有警报监控	
15	防止简单窃听或非法披露的措施(特别是在客户接待、共用空间或流动工作场所)	
16	在建筑物内指定区域内打印，或亲自打印	
17	只在规定的区域内销毁文件(例如粉碎)	
18	对于与其他公司联合使用的服务器机房，硬件(接口)采用上锁的机架、机柜或其他方式进行保护	
19	运动传感器，玻璃破碎传感器或视频监控	
20	按照告警计划及时处理告警	

如果未采取任何补充措施，请说明替代方法或原因。

（如需要，请在此补充）

1.3 不适用说明

如果物理访问控制不适用于本协议，请在如下区域简要阐明原因或提供额外补充控制说明：

（如需要，请使用附页）

2 机密性-系统访问控制

2.1 基本措施

序号	基本措施	是否已采取该措施（请填入“是”或“否”）	基本措施是必须采取的，如果未采取基本措施，请说明您的原因或替代措施
1	参照最佳实践强制使用强密码策略(例如 BSI, NIST, ENISA)		单击或点击此处输入文字。
2	密码不以纯文本形式存储的		单击或点击此处输入文字。
3	密码存储哈希值而不是原始信息		单击或点击此处输入文字。
4	IT 设施应实施授权和设备管理		单击或点击此处输入文字。
5	IT 应用程序和系统应实施授权管理		单击或点击此处输入文字。
6	只有在身份验证成功之后，才能与 IT 系统进行进一步的交互		单击或点击此处输入文字。
7	IT 系统的管理帐户只使用强密码(例如至少 15 个字符，复杂且没有常用单词成分)		单击或点击此处输入文字。
8	定义所使用的网络分段		单击或点击此处输入文字。
9	安装了杀毒软件		单击或点击此处输入文字。
10	部署了防火墙		单击或点击此处输入文字。

（如需要，请在此补充）

2.2 补充措施

除《个人信息委托处理协议》中的基本要求外，为实施系统访问控制还采取了以下哪些行动？

序号	补充措施	是否已采取该措施（请填入“是”或“否”）
1	发布员工密码规则(例如禁止披露、储存于多用途浏览器)	
2	在发生个人信息安全事件，或异常可疑情况时，锁定密码，且由用户重置密码	
3	用户凭据的安全传递(例如加密邮件，用户名和密码需不同组成字母)	
4	在多次尝试失败的情况下自动阻止访问	

5	多次尝试登录失败时，应设置登录间隔控制，特别是基于互联网访问时	
6	用户认证程序是在风险评估的基础上选择的，并考虑了潜在的攻击场景(例如从互联网直接访问的可能性)	
7	对系统访问的关键内容和管理帐户使用双因素或多因素身份验证	
8	实施中央 IT 系统以管理用户身份(身份识别与访问管理系统)	
9	定义和实施网络分段规则和程序	
10	信息按敏感级别进行分类访问	
11	系统访问账号的权限分配是否明确	
12	应用系统是否主动做过渗透测试，检测安全性	

如果未采取任何补充措施，请说明替代方法或原因。

（如需要，请在此补充）

2.3 不适用说明

如果系统访问控制不适用于本协议，请在如下区域简要阐明原因或提供额外补充控制说明:

（如需要，请使用附页）

3 机密性-授权管理

3.1 基本措施

序号	基本措施	是否已采取该措施（请填入“是”或“否”）	基本措施是必须采取的，如果未采取基本措施，请说明您的原因或替代措施
1	使用不同的个人用户帐户		单击或点击此处输入文字。
2	IT 应用系统应该实施基于角色的授权管理并存档		单击或点击此处输入文字。
3	是否满足最小必要原则：仅根据必要性(“需要知道”)和最少可能权限(“最小特权”)授权访问		单击或点击此处输入文字。
4	定期进行授权的审核(每年至少一次)		单击或点击此处输入文字。
5	审核授权并检查 IT 系统内所有用户的访问权限(例如模块、表、数据		单击或点击此处输入文字。

	集)		
6	“共享账户”的使用受到监管(例如，只有在不需要活动证明的情况下才受限制)		单击或点击此处输入文字。
7	员工职责或雇佣关系的变化立刻在其访问授权中变更调整		单击或点击此处输入文字。
8	记录读取的访问		单击或点击此处输入文字。
9	记录未授权的访问尝试		单击或点击此处输入文字。
10	定期评估系统日志		单击或点击此处输入文字。
11	对系统日志进行结合场景的评估		单击或点击此处输入文字。
12	建立并记录特权用户 ID 的管理流程(批准/更改/删除)		单击或点击此处输入文字。
13	记录特权用户帐户并定期审查		单击或点击此处输入文字。

（如需要，请在此补充）

3.2 补充措施

除《个人信息委托处理协议》中的基本要求外，为实施授权管理还采取了以下哪些行动？

序号	补充措施	是否已采取该措施 （请填入“是”或“否”）
1	用户授权管理应保存审计证据的文档	
2	用户账户的建立遵循双重控制原则的审批流程	
3	特定用户的数据不应被其他用户访问	
4	基础用户账号应实现最小权限和功能的必要性管理	
5	记录编辑的访问(包括删除/复写)	
6	系统应用级别的相关授权及角色定义是否有文档化描述	
7	相关账号是否设定可使用时长	
8	开发测试和生产环境是否分离	

如果未采取任何补充措施，请说明替代方法或原因。

（如需要，请在此补充）

3.3 不适用说明

如果授权管理不适用于本协议，请在如下区域简要阐明原因或提供额外补充控制说明:

（如需要，请使用附页）

4 机密性-加密

4.1 基本措施

序号	基本措施	是否已采取该措施（请填入“是”或“否”）	基本措施是必须采取的，如果未采取基本措施，请说明您的原因或替代措施
1	个人信息的存储是加密的		单击或点击此处输入文字。
2	所有使用的加密技术都符合最先进的技术		单击或点击此处输入文字。
3	对个人信息进行假名化处理		单击或点击此处输入文字。

（如需要，请在此补充）

4.2 补充措施

除《个人信息委托处理协议》中的基本要求外，为实施加密采取了以下哪些行动?

序号	补充措施	是否已采取该措施（请填入“是”或“否”）
1	数据的电子化传输是加密的	
2	移动设备和移动存储媒体上的所有个人信息都是加密的	
3	定义相关 IT 系统的密钥管理流程并存档	
4	端到端实施传输层加密	
5	实施了一套包含加密强度、算法和密钥管理要求的规则集	

6	假名化处理和与其他数据活动实现隔离	
7	个人信息的增删改查记录是否可查	

如果未采取任何补充措施，请说明替代方法或原因。

（如需要，请在此补充）

4.3 不适用说明

如果加密与本协议项下的服务无关联，请在如下区域简要阐明原因或提供额外补充控制说明:

（如需要，请在此补充）

5 完整性-数据传输保护

5.1 基本措施

序号	基本措施	是否已采取该措施（请填入“是”或“否”）	基本措施是必须采取的，如果未采取基本措施，请说明您的原因或替代措施
1	基于本协议同意的个人信息委托处理，定义和记录个人信息的数据受托方		单击或点击此处输入文字。
2	确保安全的物理运输(例如，安全车辆、安全容器、存储介质加密、交接协议)		单击或点击此处输入文字。
3	记录所有电子化传输个人信息的接口		单击或点击此处输入文字。
4	限制员工传输数据的权限		单击或点击此处输入文字。
5	记录基于本《个人信息委托处理协议》下的个人信息传输规则 (例如打印输出、媒体、自动传送)		单击或点击此处输入文字。

5.2 补充措施

除《个人信息委托处理协议》中的基本要求外，为实施数据传输保护采取了以下哪些行动?

序号	补充措施	是否已采取该措施（请填入“是”或“否”）
1	采用数字签名的方式保证数据传输的真实性	

2	禁用 USB 接口	
3	维护用于数据传输的虚拟专线	
4	使用所有 HTTP(S)连接必须经过的 web 代理	
5	与分支、远程办公的站点通过 VPN 连接	
6	定期查看数据接收人名单是否有变化	
7	通过技术限制仅向有权限的数据收件人转发数据	
8	在大量电子邮件分发的情况下，通过技术或组织手段防止所有收件人的信息泄露	
9	记录电子的数据传送	
10	进行了合理性、完整性和准确性检查	
11	入侵检测或入侵防御系统是否部署	
12	包含个人信息的转发日志记录是否可查	

如果未采取任何补充措施，请说明替代方法或原因。

（如需要，请在此补充）

5.3 不适用说明

如果数据传输保护与本协议项下的服务无关联，请在如下区域简要阐明原因或提供额外补充控制说明:

（如需要，请使用附页）

6 完整性-输入控件

6.1 基本措施

序号	基本措施	是否已采取该措施（请填入“是”或“否”）	基本措施是必须采取的，如果未采取基本措施，请说明您的原因或替代措施
1	输入或更改个人信息会被记录		单击或点击此处输入文字。

2	定期(无差别地)评估日志文件以检测异常输入		单击或点击此处输入文字。

6.2 补充措施

除《个人信息委托处理协议》中的基本要求外，为保证输入控件完整性采取了以下哪些行动?

序号	补充措施	是否已采取该措施（请填入“是”或“否”）
1	记录组织结构中规定的职责	

如果未采取任何补充措施，请说明替代方法或原因。

（如需要，请在此补充）

6.3 不适用说明

如果输入控件完整性与本协议项下的服务无关联，请在如下区域简要阐明原因或提供额外补充控制说明:

（如需要，请使用附页）

7 完整性-其他确保系统和服务完整性的措施

7.1 基本措施

序号	基本措施	是否已采取该措施（请填入“是”或“否”）	基本措施是必须采取的，如果未采取基本措施，请说明您的原因或替代措施
1	实施系统加固措施(例如限制/停用不必要的权限、端口、协议、服务器)		单击或点击此处输入文字。
2	多租户功能：在数据级别进行隔离		单击或点击此处输入文字。
3	基于语义标准对数据输入进行验证(语义输入验证)		单击或点击此处输入文字。
4	所有系统中保存的所有数据都会定期检查是否存在恶意软件		单击或点击此处输入文字。

7.2 补充措施

除《个人信息委托处理协议》中的基本要求外，为确保其他系统和服务的完整性采取了以下哪些行动?

序号	补充措施	是否已采取该措施（请填入“是”或“否”）

序号	补充措施	是否已采取该措施（请填入“是”或“否”）
1	由专用物理服务器实现多租户功能	
2	通过系统级别的分离实现的多租户功能	
3	有实施租户隔离的描述	
4	使用智能手机的移动设备管理解决方案	
5	针对共享虚拟机和/或应用程序实施系统加固	
6	接收到的数据和程序在打开前自动检查是否有恶意软件(访问扫描)	
7	使用数据丢失预防解决方案	
8	已经为数据字段和数据集定义了目的属性	

如果未采取任何补充措施，请说明替代方法或原因。

（如需要，请在此补充）

7.3 不适用说明

如果其他确保系统和服务完整性的措施与本协议项下的服务无关联，请在如下区域简要阐明原因或提供额外补充控制说明:

（如需要，请使用附页）

8 可用性-确保个人资料的可用性

8.1 基本措施

序号	基本措施	是否已采取该措施（请填入“是”或“否”）	基本措施是必须采取的，如果未采取基本措施，请说明您的原因或替代措施
1	有冗余的 IT 系统(终端设备、服务器、存储等)		单击或点击此处输入文字。
2	消防、电源、空调技术防护系统		单击或点击此处输入文字。
3	服务器机房和数据处理中心设有火灾和烟雾报警器		单击或点击此处输入文字。

4	服务器机房和数据处理中心设有灭火器或灭火系统		单击或点击此处输入文字。
5	服务器机房和数据处理中心有温度和湿度监测系统		单击或点击此处输入文字。
6	定期检查系统状态(监控)		单击或点击此处输入文字。

8.2 补充措施

除《个人信息委托处理协议》中的基本要求外，为确保个人资料的可用性采取了以下哪些行动?

序号	补充措施	是否已采取该措施（请填入“是”或“否”）
1	不间断电源(UPS)	
2	采用不同设计的 IT 系统(来自不同制造商的相同功能)	
3	定期检查打印件和存储介质的库存	
4	是否部署了应急灾备响应计划	
5	是否有应急计划测试文档	

如果未采取任何补充措施，请说明替代方法或原因。

（如需要，请在此补充）

8.3 不适用说明

如果个人资料的可用性与本协议项下的服务无关联，请在如下区域简要阐明原因或提供额外补充控制说明:

（如需要，请使用附页）

9 可用性-删除

9.1 基本措施

序号	基本措施	是否已采取该措施（请填入“是”或“否”）	基本措施是必须采取的，如果未采取基本措施，请说明您的原因或替代措施
1	根据数据控制者的要求，实施个人信息删除方案		单击或点击此处输入文字。
2	定义和记录处理销毁数据存储介质的流程		单击或点击此处输入文字。

9.2 补充措施

除《个人信息委托处理协议》中的基本要求外，为确保删除后的数据不可用性采取了以下哪些行动?

序号	补充措施	是否已采取该措施（请填入“是”或“否”）
1	以文档形式记录数据委托处理的删除概念	
2	按照管理规定执行数据存储介质的销毁	
3	数据删除和删除条例的完整性控制	
4	在开发、测试和生产环境实施删除	
5	碎纸机(至少 3 级，横切)用于纸质文件	
6	外部碎纸机(DIN 32757)	

如果未采取任何补充措施，请说明替代方法或原因。

（如需要，请在此补充）

9.3 不适用说明

如果确保删除后的数据不可用性与本协议项下的服务无关联，请在如下区域简要阐明原因或提供额外补充控制说明:

（如需要，请使用附页）

10 韧性-防止中断（连续性保证）

10.1 基本措施

序号	基本措施	是否已采取该措施（请填入“是”或“否”）	基本措施是必须采取的，如果未采取基本措施，请说明您的原因或替代措施
1	在所有最终用户设备上安装具有最新搜索模式的病毒扫描程序		单击或点击此处输入文字。
2	补丁管理过程(其中包括所使用软件的更新计划)		单击或点击此处输入文字。
3	使用防火墙系统(例如，在中央传输到互联网时，保护 web 服务器		单击或点击此处输入文字。

	上的数据库)		

10.2 补充措施

除《个人信息委托处理协议》中的基本要求外，为确保韧性防止系统中断采取了以下哪些行动?

序号	补充措施	是否已采取该措施（请填入“是”或“否”）
1	负载均衡器	
2	冗余的 IT 系统	
3	执行渗透测试(在 web 应用的其他应用中)	
4	规范防火墙系统的正确配置过程，包括共享/异常	
5	RAID 系统中的数据存储	
6	入侵检测系统	
7	入侵防御系统	
8	实施提高系统和服务容错能力的措施	
9	对于网站和 web 应用程序：已经定义并实现了内容安全策略(CSP)	

如果未采取任何补充措施，请说明替代方法或原因。

（如需要，请在此补充）

10.3 不适用说明

如果防止中断标准与本协议项下的服务无关联，请在如下区域简要阐明原因或提供额外补充控制说明:

（如需要，请使用附页）

11 韧性-重启和恢复可用性

11.1 基本措施

序号	基本措施	是否已采取该措施（请填入“是”或	基本措施是必须采取的，如果未采取基本措施，请说明

		“否”)	您的原因或替代措施
1	备份和重启概念(定期备份数据)		单击或点击此处输入文字。

11.2 补充措施

除《个人信息委托处理协议》中的基本要求外，为确保重启和恢复的可用性采取了以下哪些行动?

序号	补充措施	是否已采取该措施（请填入“是”或“否”）
1	采用合适的物理存储来备份介质(例如安全、防火、空间隔离)	
2	适当保护备份免受勒索软件的加密	
3	重新启动概念(在系统发生故障时采取立即恢复可用性的措施)	
4	记录和测试的应急操作概念(IT 服务连续性)	
5	记录和建立业务连续性管理	

如果未采取任何补充措施，请说明替代方法或原因。

（如需要，请在此补充）

11.3 不适用说明

如果重启和恢复可用性标准与本协议项下的服务无关联，请在如下区域简要阐明原因或提供额外补充控制说明:

（如需要，请使用附页）

12 组织措施及流程-组织安全措施

12.1 基本措施

序号	基本措施	是否已采取该措施（请填入“是”或“否”)	基本措施是必须采取的，如果未采取基本措施，请说明您的原因或替代措施
1	在公司内部有针对数据安全领域的角色和职责的描述及人员配备，以及对岗位的充分理解		单击或点击此处输入文字。
2	实施适当的信息安全管理系统		单击或点击此处输入文字。

3	是否存在足够的事件管理(对安全漏洞的响应)		单击或点击此处输入文字。
4	设置攻击识别和报告(事件响应)		单击或点击此处输入文字。
5	收集有关所使用的系统和软件(资产)的技术漏洞信息，并根据影响进行评估		单击或点击此处输入文字。
6	根据数据保护需求(如机密性、可用性、完整性)对所有信息进行分类		单击或点击此处输入文字。
7	在测试和开发环境中只处理合成数据，即不处理真实个人信息		单击或点击此处输入文字。
8	禁止在源代码(存储库)中存储个人信息		单击或点击此处输入文字。
9	定期验证信息和 IT 系统的使用目的(例如由 IT security 或数据保护办公室进行使用目的审计)		单击或点击此处输入文字。
10	定期审查所有保护措施的有效性，并在适当情况下进行适当调整(PDCA 循环)		单击或点击此处输入文字。

12.2 补充措施

除《个人信息委托处理协议》中的基本要求外，组织安全措施还采取了以下哪些行动?

序号	补充措施	是否已采取该措施 （请填入“是”或“否”）
1	内部定义了信息处理的安全准则，由管理层采用并传达给员工	
2	在当前协议的背景下执行 IT 系统文档变更管理流程	
3	为所有用户提供有关数据保护和数据安全的意识培训	
4	提供数据保护方面的培训或适当的内部教育	
5	生产系统和开发/测试系统的分离	
6	制定了员工移动/私人使用终端设备(例如智能手机、笔记本电脑)的规定	
7	公司是否有法务部及信息技术部的设立	
8	是否有相关信息安全管理资质：比如 ISO27001，等级保护认证 GB/T 22239，请一并提供资质证明）	
9	是否定义了相关个人信息安全事件处理实施流程	

如果未采取任何补充措施，请说明替代方法或原因。

（如需要，请在此补充）

12.3 不适用说明

如果组织安全措施标准与本协议项下的服务无关联，请在如下区域简要阐明原因或提供额外补充控制说明:

（如需要，请使用附页）

13 组织措施及流程-监控分配

13.1 基本措施

序号	基本措施	是否已采取该措施（请填入“是”或“否”）	基本措施是必须采取的，如果未采取基本措施，请说明您的原因或替代措施
1	以达成本协议为目的，记录所有用于处理个人信息的子处理器		单击或点击此处输入文字。

13.2 补充措施

除《个人信息委托处理协议》中的基本要求外，在监控分配中采取了以下哪些行动?

序号	补充措施	是否已采取该措施（请填入“是”或“否”）
1	和其他委托处理方的服务协议中应继承同样水平的服务水平协议（SLA）	
2	在相关子处理节点有质量管理体系完全满足数据委托处理	
3	在相关子处理节点之间有信息安全管理系统(ISMS)可以完全覆盖数据委托处理	
4	所有相关子处理节点均已在信息安全领域建立认证(例如 ISO 27001, TISAX, SOC 2, BSI IT-Grundschutz)	
5	通过提交自我评估，定期监测相关的子处理者	
6	定期对相关子处理节点进行第三方检查(如审核员、数据保护审核员)	
7	通过检查与(进一步)相关子处理节点签订的合同，定期检查相关子处理节点	
8	对分包商实施检查	
9	存在数据委托处理的内部政策和工作指示	

如果未采取任何补充措施，请说明替代方法或原因。

（如需要，请在此补充）

13.3 不适用说明

如果监控分配标准与本协议项下的服务无关联，请在如下区域简要阐明原因或提供额外补充控制说明:

（如需要，请使用附页）

问卷 C. 批准分包商（如适用）

1 批准分包商

分包商名称、地址	
名称	单击或点击此处输入文字。
地址	单击或点击此处输入文字。
联系人	单击或点击此处输入文字。
联系方式	单击或点击此处输入文字。

2 分包商职能的简要描述

单击或点击此处输入文字。

（提供有关分包商的其他详细信息）

受托方应确保，上述分包商受**《个人信息委托处理协议》**所列义务的约束采取了问卷 B 中所列的数据保护及信息安全措施。