ESET Inspect Cloud

0

单击此处显示此文档的联机版本

Digital Security
Progress. Protected.

ESET Inspect Cloud 由 ESET, spol. s r.o. 开发

有关详细信息，请访问 https://www.eset.com

技术支持https://support.eset.com

修订日期 2024年m月12日

ESET Inspect Cloud

ESET Inspect Cloud 既有其本地版本的所有强大功能，又有云交付服务易于部署和几乎无维护要求的优点。它是 ESET Endpoint 检测技术和专业知识的结晶。

它有一个包含近 1,000 条规则的完全透明且可自定义的规则引擎，由 ESET 的顶级恶意软件研究人员编写，用于检测与 MITRE ATT&CK 框架交叉引用的威胁和行为异常。

对于响应和修复，ESET Inspect Cloud 为安全专业人员提供了多种功能：

- 阻止可执行文件
- 终止进程
- 将端点与网络隔离
- 终端远程外壳

所有响应操作都可以手动触发，也可以在预定义的响应场景下自动触发。

通过事件管理系统可以轻松处理事件，而借助强大的威胁指标 (IoC) 搜索和筛选功能，威胁搜寻变得轻而易举。

ESET Inspect Cloud 包括本地版 ESET Inspect 的所有关键特性和功能，但略有调整以适应基于云的管理需求。

- Windows、macOS 和 Linux 多平台支持可监控几乎任何端点，从而为组织提供全面保护，而不管其平台类型如何。
- 支持 ESET 企业版产品（版本 6 及更高版本）。
- 许可证管理完全在 ESET Business Account 中完成。创建一个新的 ESET PROTECT Cloud 和 ESET Inspect Cloud 实例。单个实例最多支持 25,000 个端点。
- 面板不包含**服务器状态**和**事件加载**选项卡（无需维护）。
- **设置**部分包含的配置选项少于本地版 ESET Inspect Cloud，因为无需 ESET Inspect Database 维护。
- **设置**部分提供搜索引擎集成、规则学习模式和指定 ESET Inspect Cloud 实例名称的选项。
- 数据收集配置为存储最重要的数据。虽然会存储与进程相关的所有数据，但低级别事件的收集仅限于可疑事件。

ESET 状态门户会显示 ESET 云服务的当前状态、计划中断和过去的事件。如果您在使用支持的 ESET 服务时遇到问题，但在“状态门户”中未看到该问题列出，请联系 ESET 技术支持。

监视小组会在内部核实潜在问题，然后手动发布和更新已确认的事件，以保持较高的可信度和准确性。因此，它们在“状态门户”上显示略有延迟。如果在手动确认之前就解决了持续时间较短的事件，则可能不会发布这些事件。

可用性

我们的目标是提供 99.5% 的服务可用性。我们的努力和定义明确的流程会推动实现这一目标。

如果 ESET Inspect Cloud 服务中断，端点仍保持安全且不受影响。

更改日志

此页面显示 ESET Inspect Cloud 的更改日志（最多显示最近十个版本，最新版本位于顶部）。更改日志仅提供英文版。另请参阅 ESET 产品的发布日期和最新版本

Version 1.11.2882.0

- Fixed: performance issues
- Fixed reliability issues

Version 1.11.2872.0

- New: Incident Visualizations
- New: Automated Resolution for Detections
- New: Utilizing SHA Hashes for Script Exclusions
- New: Exclusions Enabled by Default
- Improved: Faster Loading of Detections and Incidents Details
- Improved: Faster Rule Execution for Historical Data
- Improved: Table Filtering Improvements
- New: Diagnostics Data Collection
- New: New Detection Rules

Version 1.10.2664.0

- Added: Multitenancy support completed (management of access rights per group, synchronization of static group types, and improved blocking of modules)
- New: New signals to indicate ransomware attacks
- New: Simple incident creation based on the SIEM rules
- New: Detection of files delivered through RDP connection's copy & paste
- New: Displayed OS API calls from LiveGuard

- New: MDR Report Template
- New: Dark Mode
- New: ESET LiveGuard information columns in the executables table view
- Fixed: Stability and performance fixes

Version 1.9.2423.0

- Improved: Optimization of memory usage caused by operation's cache in ESET Inspect Connector
- proved: Option to Submit selected executables to LiveGuard in the "Executables" view
- FixedIm: Performance, stability and memory issues
- Fixed: Rules actions operability and exporting issues

Version 1.9.2404.0

- New: Multitenancy for selective Access Rights control and targeting of e.g. Detection Rules per tenant
- New: Integration with LiveGuard Advanced cloud sandbox
- Added: Ability to Report Incident as an action available in the Rules syntax
- Added: Ability for Endpoint Detection types to be matched in the EI Rules (for elevation to Incident)
- Added: Monitoring of selected Win API calls
- Added: Canary files utilization for enhanced detection of Ransomware behaviors
- Improved: Detection of multiple similar network events in a row (previously considered as "duplicates")
- Improved: Signals about potentially suspicious events from Firewall and Network protection layers
- Added: Ability to detect events of writing to and modifying multiple files
- Added: Link between URL connections and dropped files (for improved investigation of Incidents)
- Added: Ability to detect setting file attributes ("SetFileAttribute") on Linux
- Added: Ability to detect and investigate a process deleting its files
- Added: REST API now enables Incident Management capabilities
- Added: REST API now allows searching for Executables and their metadata
- Added: User Logout as a new action
- Added: Submit files to LiveGuard Advanced analysis as a new action
- Added: "Remember this device" for login when using 2FA
- Improved: Database and general performance

- Improved: Executable certificate signature verification method

Version 1.8.2218.0

- Fixed: EI Connector crashes when connecting via Remote Terminal
- Fixed: EI Connector crashes when printing errors
- Fixed: Update to v1.8 failing due to lack of disk space

Version 1.8.2214.0

- Fixed: Memory Leaks
- Fixed: EI Connector not running on Ubuntu 22.04
- Fixed: Rule triggering on Linux
- Improved: Console log-in performance
- Added: Incidents data synchronization with ESET PROTECT for new Incidents dashboard
- Added: Event filtering based on "FileAttribute"

Version 1.8.2211.0

- Changed: Moving of Detection Rules evaluation from ESET Inspect Cloud to individual endpoints
- Added: ESET MSP Administrator integration
- Improved: Partitioning of Processes table
- Added: Display Purge status overview
- Added: Ability to monitor SYS Files
- Added: Ability to monitor Kernel module load/unload operations on Linux
- Improved: Computer Reboot and Shutdown exposed to Rule engine as response actions
- Changed: Alignment of context menus and toolbars to match ESET PROTECT
- Improved: Ability to go from Process's raw events to Computer's raw events
- New: ISO certification achieved for ESET Inspect Cloud

Version 1.7.1991.0

- Added: Support for EI Agent configuration by installer using policy file
- Added: Hardening of EI Cloud security
- Added: Ability to invoke Product Tour ("Onboarding Wizard") on-demand from Help menu
- Changed: Default filter in Computers view to also show Computers without EI Connector

- Fixed: Issue with some Exclusions not working correctly
- Fixed: Issue of unknown connection ID being received for some events
- Fixed: The "Select rule actions" dialog in Remediation menu not resetting choices correctly
- Fixed: Issue with Computer events process filter losing its value when the page is reloaded
- Fixed: Incorrect heading and Online Help links in the Onboarding Wizard
- Fixed: The "License" link in Help
- Fixed: Incorrect operation type being displayed for some Rule based Detections
- Fixed: The Detection Info filter in Detections view not behaving correctly
- Fixed: Issue with EI Connector for Linux requiring to be restarted after upgrade
- Fixed: "Assignee" filter in Incidents view incorrect behavior
- Fixed: Connectivity issues when used with Proxy
- Fixed: Issue with optional Rules being incorrectly disabled after upgrade
- Fixed: Rules that should not be enabled being enabled unexpectedly
- Fixed: Landing page design for invalid redirects
- Fixed: Sync issue between EPC and EIC related to static groups/computers/metadata/alerts
- Fixed: Performance degradation of event processing in large environments
- Fixed: Inconsistencies between EPC and EIC authorization (user permissions) pop-ups
- Fixed: Issue with ability to download scripts on Linux
- Fixed: Issue with Rerun task not showing results when used on a disabled Rule

Version 1.7.1978.0

- Added: Product renaming
- Added: Linux support - EI Connector available for multiple major Linux distributions
- Added: Ability to add Response/Remediation actions to Detection Rules via graphical interface
- Added: Ability to add "Kill Process" response action to Rules
- Added: Tagging of actions done by ESET Services Representatives
- Added: Removal of inconsistencies between ESET PROTECT and Inspect
- Added: Hint (tooltip) for Trigger Event column
- Added: Onboarding Wizard

- Added: Ability to invoke database purge on demand
- Changed: Terminal (remote PowerShell) limited to 2FA enabled users
- Improved: Response/Remediation menu in Detection Details view
- Improved: Improved Automatic Exclusions UI (Questions view)
- Improved: Unification of visibility for user created objects (Searches, Tasks, Incidents)
- Improved: Visibility of Incident description

使用限制和数据保留策略

大小调整

ESET Inspect Cloud 目前支持每个实例最多 25,000 个端点。如果有更多端点需要保护，请考虑将环境划分为多个 ESET Inspect Cloud 和 ESET PROTECT 实例。例如，根据组织的多个物理位置或分支划分。或者，考虑使用本地版 ESET Inspect该版本支持更多数量的端点（使用计算器针对您的环境缩放 ESET Inspect

---

数据保留

ESET Inspect Cloud 在轻量级模式下运行。因此，数据收集类型设置为存储最重要的数据

- 原始事件的保留期为 7 天。比这更旧的记录将被永久移除。
- 检测的保留期为 31 天。比这更旧的记录将被永久移除。

检测在添加到事件中后不会被删除。

数据库限制

所有事件都实施了字符限制，以限制数据库的增长。这些字符限制设置为 260。

先决条件

必须允许网络防火墙中的出站连接ESET Inspect Cloud 才能正常工作：

域	端口类型/端口号	说明
eba.eset.com	TCP/443	ESET Business Account
ema.eset.com	TCP/443	Managed Service Provider
msp.eset.com	TCP/443	Managed Service Provider
identity.eset.com	TCP/443	ESET 身份认证服务器
inspect.eset.com	TCP/443	ESET Inspect Cloud
eu01.inspect.eset.com	TCP/443	ESET Inspect Cloud Web 控制台位置：欧洲

域	端口类型/端口号	说明
us01.inspect.eset.com	TCP/443	ESET Inspect Cloud Web 控制台位置：美国
jp01.inspect.eset.com	TCP/443	ESET Inspect Cloud Web 控制台位置：日本
eu01.agent.edr.eset.systems 或 IP 52.166.186.239	TCP/8093	位置：欧洲
us01.agent.edr.eset.systems 或 IP 40.83.252.19	TCP/8093	位置：美国
jp01.agent.edr.eset.systems 或 IP 20.188.24.252	TCP/8093	位置：日本

在 ESET Connect 联机帮助中查找 **ESET Connect** 的网络先决条件。

开始使用 ESET Inspect Cloud

ESET Inspect Cloud 可立即使用，摒弃了本地解决方案所需的安装和设置步骤。它易于部署和使用。这项新的云托管服务附带一个基于 Web 的管理控制台（ESET Inspect Cloud Web 控制台），您可以通过适当的 Internet 连接从任何位置或设备以虚拟方式连接该控制台。

创建 ESET Inspect Cloud 实例的两种方法：

- 使用 ESET Business Account 的 ESET Inspect Cloud
- 使用 Managed Service Provider 管理员的 ESET Inspect Cloud

激活 ESET Inspect Cloud 所需的许可证

需要符合条件的许可证才能直接从 ESET Business Account 的面板或 ESET Managed Service Provider 门户激活 ESET Inspect Cloud。

有关符合条件的许可证的详细信息，请联系您当地的 ESET 合作伙伴。

ESET PROTECT Cloud 必需

ESET Inspect Cloud 与 ESET PROTECT Cloud 绑定，因此在没有 ESET PROTECT Cloud 的情况下无法激活。

使用 ESET Business Account 的 ESET Inspect Cloud

按照 ESET Business Account 用户指南设置 ESET Inspect Cloud 实例。

若要正确使用通过 ESET Business Account 激活的 ESET Inspect Cloud，需要满足这些先决条件。

使用 Managed Service Provider 管理员的 ESET Inspect Cloud

如果您是 MSP 计划的 ESET 合作伙伴，请遵循 Managed Service Provider 管理员用户指南。

若要正确使用通过 Managed Service Provider 激活的 ESET Inspect Cloud，需要满足这些先决条件。

安装 ESET Inspect Connector

ESET Inspect Connector 安装在 ESET Inspect Cloud 监控的端点设备上，收集 ESET Inspect Cloud 的数据、删除恶意组件和阻止这些组件的执行。

请参阅安装/部署主题中的 ESET Inspect Connector 安装过程。

ESET Inspect Cloud Web 控制台

ESET Inspect Web Console 是一款功能强大的用户界面，让您可以与 ESET Inspect Cloud 交互并充分利用端点检测和响应 (EDR) 解决方案。有关详细信息，请参阅开始使用 ESET Inspect Web Console 主题。

ESET Inspect Cloud 的安全性

介绍

本文档的目的是概述在 ESET Inspect Cloud 中应用的安全实践和安全控制。安全实践和控制旨在保护客户信息的机密性、完整性和可用性。请注意，安全实践和控制可能会发生变化。

范围

本文档讨论的范围是针对以下对象概述安全实践和安全控制ESET Inspect Cloud 基础架构、组织、人员和操作过程。安全实践和控制包括：

1. 信息安全策略
2. 信息安全组织
3. 人力资源安全
4. 资产管理
5. 访问控制
6. 加密
7. 物理和环境安全
8. 操作安全
9. 通信安全
10. 系统获取、开发和维护
11. 供应商关系
12. 信息安全事件管理
13. 业务连续性管理的信息安全方面
14. 合规性

安全概念

ESET, spol. s r.o. 公司已通过 ISO 27001:2013 认证，集成的管理系统范围明确涵盖 ESET Inspect Cloud 服务。

因此，信息安全的概念在对网络层、操作系统、数据库、应用程序、人员和操作流程应用安全控制时，使用 ISO 27001 框架来实施分层防御安全策略。应用的安全实践和安全控制旨在相互重叠和互补。

安全实践和控制

1. 信息安全策略

ESET 使用信息安全策略来涵盖 ISO 27001 标准的各个方面，包括信息安全监管以及安全控制和实践。每年都会对策略审阅并在发生重大更改后更新，以确保其持续适用性、充分性和有效性。

ESET 会对本策略执行年度审阅和内部安全检查，以确保与本策略保持一致。对于 ESET 员工而言，违反信息安全策略会受纪律处分；对于供应商而言，违反信息安全策略会支付违约金，甚至于终止合同。

2. 信息安全组织

ESET Inspect Cloud 的信息安全组织由多个参与信息安全和 IT 的团队和个人组成，包括：

- ESET 行政管理
- ESET 内部安全团队
- 业务应用 IT 团队
- 其他支持团队

信息安全责任会根据现有信息安全策略进行分配。将对内部过程进行识别并评估，以查找是否存在任何未经授权、意外修改或滥用 ESET 资产的风险。内部过程中有风险或敏感的活动会采用职责划分原则来降低风险。

ESET 法律团队负责就网络安全和个人数据保护与政府机构（包括斯洛伐克监管机构）联系ESET 内部安全团队负责联系特殊利益团体，例如 ISACAESET 研究实验室团队负责与其他安全公司和较大的网络安全社区进行沟通。

在已应用项目管理框架（从概念到项目实现）的项目管理中，会对信息安全加以考虑。

通过使用在移动设备上实施的策略来涵盖远程工作和远程办公，其中包括在通过不受信任的网络漫游时在移动设备上使用强加密数据保护。移动设备上的安全控制旨在独立于 ESET 内部网络和内部系统工作。

3. 人力资源安全

ESET 使用标准的人力资源实践，包括旨在确保信息安全的策略。这些实践涵盖整个员工生命周期，适用于访问 ESET Inspect Cloud 环境的所有团队。

4. 资产管理

ESET Inspect Cloud 基础架构包含在 ESET 资产清单中，并根据资产类型和敏感度应用了严格的所有权和规则ESET 定义了内部分类方案。所有 ESET Inspect Cloud 数据和配置都归类为机密信息。

5. 访问控制

ESET 的访问控制策略管理 ESET Inspect Cloud 中的每个访问。访问控制是基于基础架构、网络服务、操作系统、数据库和应用程序级别设置的。应用程序级别上的完全用户访问管理是自主的（使用了 Microsoft Azure 基于角色的访问控制）。

ESET 后端访问严格限于获得授权的个人和角色。用于用户（取消）注册、（取消）配置、权限管理和查看用户访问权限的标准 ESET 过程，可用于管理 ESET 员工对 ESET Inspect Cloud 基础架构和网络的访问。

强身份验证已启用，可保护对所有 ESET Inspect Cloud 数据的访问。

6. 加密

为了保护 ESET Inspect Cloud 数据，强加密功能用于对静态数据和传输中的数据进行加密。

7. 物理和环境安全

ESET Inspect Cloud 是基于云的产品。ESET 依赖私有云和 Microsoft Azure 云。私有云数据中心的物理位置完全位于欧盟 (EU)。Microsoft Azure 不限于欧盟境内；但是，它仅用于存储从提交的文件创建的单向哈希，不会包括个人数据。强加密功能已启用，来保护传输过程中的客户数据。

8. 操作安全

ESET Inspect Cloud 服务是基于严格操作程序和配置模板自动运维的。所有更改（包括配置更改和新程序包部署）都必须事先得到批准并在专用测试环境中进行测试，然后才能部署到生产中。开发、测试和生产环境彼此隔离。ESET Inspect Cloud 数据仅存在于生产环境中。

ESET Inspect Cloud 环境通过操作监视来进行监管，以快速识别问题并为网络和主机级别的所有服务提供足够容量。

所有配置数据都存储在我们定期备份的存储库中，以便自动恢复环境的配置。ESET Inspect Cloud 数据备份会同时存储在本地和异地。

备份会被加密，并定期测试其可恢复性（作为业务连续性测试的一部分）。

将根据内部标准和准则对系统执行审核。将持续收集来自基础架构、操作系统、数据库、应用程序服务器和安全控件的日志和事件。日志会由 IT 和内部安全团队进一步处理，以识别操作和安全异常以及信息安全事件。

ESET 使用常规技术漏洞管理过程来处理 ESET 基础架构（包括 ESET Inspect Cloud 和其他 ESET 产品）中出现的漏洞。这一过程包括主动漏洞扫描以及对基础架构、产品和应用程序的重复渗透测试。

ESET 规定了内部基础架构、网络、操作系统、数据库、应用程序服务器和应用程序安全的内部准则。这些准则通过技术合规性监视和我们的内部信息安全审核计划进行检查。

9. 通信安全

ESET Inspect Cloud 环境通过原生云段进行分段，网络访问仅限于网段之间的必要服务。网络服务的可用性是通过可用性区域、负载平衡和冗余等原生云控制来实现的。专用的负载平衡组件已部署，来为强制执行通信和负载平衡授权的 ESET Inspect Cloud 实例路由提供特定端点。持续监控网络通信以发现操作和安全异常。潜在的攻击可以通过使用原生云控制或部署的安全解决方案来解决。所有网络通信都通过常用技术（包括 IPsec 和 TLS）加密。

10. 系统获取、开发和维护

ESET Inspect Cloud 系统的开发是根据 ESET 安全软件开发策略进行的。内部安全团队从初始阶段就包含在 ESET Inspect Cloud 开发项目中，对所有开发和维护活动不予理会。在软件开发的各个阶段，内部安全团队会定义安全要求并检查其满足情况。所有服务（包括新开发的服务）的安全性会在发布后持续进行测试。

11. 供应商关系

相关的供应商关系是根据有效的 ESET 准则构建的，该准则涵盖了从信息安全和隐私角度来看的整个关系管理和合同要求。定期评估关键服务提供商所提供服务的质量和安全性。

此外，ESET 会利用 ESET Inspect Cloud 的可移植性原则来避免出现供应商锁定。

12. 信息安全管理

ESET Inspect Cloud 中的信息安全事件管理的执行方式与其他 ESET 基础架构类似，并依赖已定义的事件响应程序。事件响应中的角色在多个团队（包括 IT、安全、法律、人力资源、公共关系和行政管理）中定义和分配。某个事件的事件响应团队是由内部安全团队根据事件分类建立的。该团队会进一步与处理该事件的其他团队进行协调。内部安全团队还负责收集证据和吸取教训。将向受影响的各方传达事件发生和解决方案。如有必要，ESET 法律团队会负责根据《一般数据保护条例 (GDPR)》和《网络安全法案》（取代《网络和信息安全指令 (NIS)》）通知监管机构。

13. 业务连续性管理的信息安全方面

ESET Inspect Cloud 服务的业务连续性采用健壮架构编写，用于最大程度地提高所提供服务的可用性。如果 ESET Inspect Cloud 组件或 ESET Inspect Cloud 服务的所有冗余节点发生灾难性故障，则可以从异地备份和配置数据完全恢复。定期测试恢复过程。

14. 合规性

与 ESET 的其他基础架构和过程类似，定期评估和审查 ESET Inspect Cloud 的法规和合同要求的合规性，并采取必要的步骤以持续确保合规性。ESET 已注册为云计算数字服务的数字服务提供商，涵盖多项 ESET 服务（包括 ESET Inspect Cloud）。请注意，ESET 合规性活动并不一定意味着客户的整体合规性要求因此等到满足。

使用条款

自 2023 年 9 月 25 日起生效 | 请参阅以前版本的使用条款 | 比较更改

这些使用条款（“条款”）构成 ESET, spol. s r. o.（注册办公室位于Einsteinova 24, 85101 Bratislava, Slovak Republic，业务识别号31333532，“ESET”或“提供商”）与您（作为自然人或法人（“您”或“用户”），可访问管理帐户，ESET Inspect Cloud 和 ESET 所拥有并提供的联机服务（“帐户”），这些联机服务都在可通过 ESET 联机帮助访问的适用文档（“文档”）中进行具体说明）之间的特定协议。如果您代表某个组织使用帐户，即表示您同意该组织的条款并且保证您拥有授权使该组织受这些条款的约束。在此情况下，“用户”和“您”指该组织。请仔细阅读这些条款。它们还与通过ESET提供的服务相关或与帐户相关。有关使用这些条款之外的单个服务的特殊条件已在每个服务中进行了声明，并且接受这些条件构成服务激活过程的一部分。

安全和数据防护

帐户可提供对 ESET 所提供的服务的访问。帐户的注册和使用以及提供和维护通过帐户访问的服务需要用户提供完整姓名、公司名称、国家/地区、有效的电子邮件地址、电话号码、许可数据和统计数据。您在此同意将数据收集并传输到提供商的服务器或其合作伙伴的服务器，其目的是确保帐户的功能、授权使用帐户以及保护提供商的权利。本条款缔结后，提供商或其合作伙伴有权传输、处理和存储能够识别您的重要数据，用于支持目的和本条款的履行。您仅授权根据本条款、个人服务条款和文档中指定的用途和方式使用帐户。

您有责任确保帐户和用于登录的凭据的安全。ESET 对您因未遵守维护安全的义务而造成的任何损失或损害概不负责。用户也要对与使用帐户有关的任何活动负责，无论是否得到授权。如果帐户被盗用，请立即通知提供商。

为了您的帐户能够正常工作，需要收集和处理有关受监视端点设备和网络的数据（“数据”）。在基础架构中执行的监视范围以及收集的确切数据完全取决于您和您的管理员管理的规则、排除项和设置。因此，我们将根据附件 2 中提供的《数据处理协议》以及我们的《隐私政策》以数据处理者的身份处理数据，仅向您提供帐户和相关服务及功能。

根据本条款，您在理解提供商将保持透明度、道德标准和法律合规性的情况下，承认网络安全在动态数字

环境中的重要性，并同意持续监视和分析必要的数据，以增强和调整网络安全策略、检测和抵制恶意活动、查明漏洞并持续改进安全措施和服务本身，包括将数据用于这些目的。同意本条款即表示您授权将数据用于指定目的，并确认知悉提供商对维护安全环境的承诺。我们在处理数据和实施必要的安全措施时将遵守相关的隐私和数据保护法规。

数据以及与帐户有关的其他日志应按照文档中提供的《日志保留策略》进行存储。

关于隐私、个人数据保护和作为数据主体所拥有权利的详细信息可以在隐私政策中找到。

API 数据安全性

使用应用程序编程接口“API”即表示您确认并同意传输到 API 或从 API 接收的任何数据或信息可能会离开或进入 ESET 的安全基础架构。这包括但不限于从第三方系统或网络接收的指令、请求、命令或指示。您明白 ESET 无法保证传输到 API 或由 API 接收的数据或信息的安全性或机密性，并且 ESET 对此类数据或信息的任何未经授权的访问、披露、丢失、损坏或滥用概不负责。

您声明并保证已采取适当的安全措施，来保护传输到 API 的数据和信息，以及通过 API 接收自第三方的任何指令。您同意对离开或进入 ESET 基础架构的数据和信息的安全性和机密性以及通过 API 接收的任何指令的解释和执行全权负责。您确认承担 API 与第三方系统或网络交互的所有相关风险，包括但不限于恶意干扰的风险。

公平使用策略

您必须遵守文档中规定的技术限制。您同意将仅以不会限制其他用户获取这些服务的可能性的方式使用该帐户及其功能。提供商保留限制向个别用户提供的服务范围的权利，以确保最大数量的用户能够使用服务。限制服务范围还将意味着完全杜绝使用帐户的任何功能和删除数据及信息的可能性。

提供商还保留有限制帐户管理的设备数量的权利。允许您添加和管理 25.000 台端点设备。

使用限制

帐户仅限用于 ESET PROTECT Enterprise Bundle 中的产品。要创建 ESET Inspect Cloud 实例，应使用 ESET Business Account。

特殊服务

如果您（自行决定）从 ESET 获得免费访问和使用其产品、服务或特定功能的权利，或者您从 ESET 获得访问和使用标记为“Beta”“抢先体验”、“预发布”或由 ESET 类似地标记为未经测试、实验性或未完成的服务、产品或功能（“特殊服务”）的权利，本节的规定应适用于您对此类特殊服务的使用，如果与本条款的规定有任何冲突，应以本节的规定为准。

您确认知悉，特殊服务可能包含一些错误和缺陷，它们可能导致特殊服务出现故障以及导致损害（包括系统故障、中断或数据丢失）。如果ESET提供与特殊服务相关的任何更新、帮助或任何技术支持，这些更新、帮助或技术支持的提供仅由 ESET 自行决定，并且可能随时中止。ESET 没有义务存储通过特殊服务收集的数据或其他信息，并且可以在无事先通知的情况下将其删除。您还确认知悉，在相关特殊服务正式发布之前，可能无法获得特殊服务的文档。

特殊服务应在已接受订单或者您获得访问和使用特殊服务的权利所依据的其他文档或通信中规定的期限内提供。但是，ESET 有权随时自行决定停止提供特殊服务或其任何功能。在这种情况下，ESET 应在终止提供特殊服务前至少三十（30）天向您发送事先通知，除非由于重要的商业、技术和安全等原因而无法实施该行为。

位置

提供商可能允许您选择可用的帐户托管位置，包括提供商选择的推荐位置。您确认，如果选择建议位置外的其他位置，您的用户体验可能会受到影响。根据所选位置，本协议的附件 2 中包含的数据保护协议和本协议的附件 3 中包含的标准合同条款可能适用ESET 保留随时更改特定位置的权利（恕不另行通知），为了改善 ESET 根据您的位置偏好（例如欧盟）提供的服务。

软件

ESET 和/或其各供应商拥有或可能使用在帐户网站上可用的所有软件的版权（以下简称“软件”）。本软件只能根据最终用户许可协议（以下简称“EULA”进行使用EULA 与软件一起提供，或者是其中一部分。在用户未同意 EULA 时，不能安装随 EULA 一起提供的软件。有关许可、版权、文档和商标的其他信息已在法律信息中进行规定。

限制

您不得复制、分发、提取组件或创建帐户的衍生版本。使用帐户时，您必须遵守以下限制：

(a) 您不得以本条款明确提供的方式以外的任何其他方式使用、修改、翻译、复制帐户或转让帐户或其组件的使用权。

(b) 您不得出售帐户、授予从属许可、将帐户出租给他人，或从他人处租用帐户或借出帐户，或者将帐户用于提供商业服务。

(c) 您不得在法律明确禁止此类限制的范围之外以任何其他方式反向工程、反编译、反汇编帐户，或试图获得帐户的源代码。

(d) 您同意使用帐户的方式必须符合有关帐户使用的相关法律中的所有适用法规，包括但不局限于符合版权法和其他知识产权中适用的限制。

免责声明

作为用户，您特此确认帐户以及服务不带任何明示或暗示担保且在适用法律允许的最大范围内“按原样”提供。提供商、其许可提供商或分支机构或者版权所有者都不得提供任何明示或暗示的陈述或保证，包括但不限于适销性保证、特定用途适用性保证、对该帐户或服务不侵犯任何第三方专利、版权、商标或其他权利的保证。提供商或任何其他方均不保证该帐户或服务符合您的要求，或该帐户或服务操作将顺畅无误。为实现预期目的而选择和使用帐户和服务以及从中所获结果的全部责任和风险由您承担。

除这些条款特别列出的义务以外，这些条款不对提供商及其许可提供商施加任何其他义务。

责任限制

在适用法律允许的最大范围内，任何情况下提供商、其员工或合约商均不对以下损失负责：以任何形式造成的任何赢利、收入或销售额损失，任何数据损失，为获得备用物品或服务支付的额外费用，财产损失、人身伤害，营业中断，商业信息损失，或任何特殊、直接、间接、意外、经济、涵盖、犯罪、特殊或后继损失。无论这些损失是由合约、故意误操作、疏忽或其他责任理论造成，还是因使用或无法使用帐户导致，提供商、其员工或合约商均不负责，即使已经通知提供商或其许可提供商或分支机构此类损失的可能。由于某些国家/地区和司法管辖区不允许免除责任，但可能允许限制责任，在这种情况下，提供商、其员工、合约商或附属公司的责任应限制为您购买有问题的服务或帐户所支付的价格。

贸易控制合规性

(a) 您将不得直接或间接地向任何人出口、再出口、转让或以其他方式提供该软件，不得以任何方式使用该

软件，也不得涉及任何行为，否则可能导致 ESET 或其控股公司、其子公司及其任何控股公司的子公司以及由其控股公司控制的实体（“关联公司”）违反《贸易管制法》或承担《贸易管制法》所规定的不良后果，包括：

i. 美国、新加坡、英国、欧盟或其任何成员国的任何政府、州或监管机构、将履行这些条款规定义务的国家/地区、成立或运维 ESET 或其任何关联企业的国家/地区颁布或通过的针对出口、再出口或转让商品、软件、技术或服务进行控制、限制或施加许可要求的任何法律，和

ii. 美国、新加坡、英国、欧盟或其任何成员国的任何政府、州或监管机构、将履行这些条款规定义务的国家/地区、成立或运维ESET或其任何关联企业的国家/地区实施的任何经济、金融、贸易或其他方式的制裁、限制、禁运、进出口禁令、禁止转移资金或资产或提供服务或其他等效措施（上述“i.”和“ii.”部分中提到的法律行为统称为“《贸易管制法》”）。

(b) 如果发生以下情况，ESET 有权立即中止或终止这些条款所规定的义务：

i.ESET 合理认为用户已违反或可能违反了这些条款中本贸易控制合规性条款的第 (a) 部分的规定；或

ii. 最终用户和/或软件受《贸易管制法》约束，因此 ESET 合理认为继续履行这些条款所规定的义务可能会导致 ESET 或其关联公司违反《贸易管制法》，或承担《贸易管制法》所规定的不良后果。

(c) 这些条款无意，也不应理解或解释为诱导或要求任何一方以不遵循《贸易管制法》、受《贸易管制法》处罚或禁止的方式行事或不作为（或者同意行事或不作为）。

管辖法律和语言

这些条款受斯洛伐克法律管辖，并按斯洛伐克法律解释。最终用户和提供商同意，法律与联合国国际货物销售合同公约之间的冲突原理不适用。如果您是在欧盟有惯常居所的消费者，您还可以通过您居住国的适用法律的强制性规定获得额外保护。

您明确同意，对于与提供商的任何索赔或争议或与您使用软件、帐户或服务有关的或由这些条款或特殊条款（如果适用）引起的任何索赔或争议的专属管辖权属于斯洛伐克布拉迪斯拉发第一地区法院，并且您进一步赞成并明确同意斯洛伐克布拉迪斯拉发第一地区法院作出的有关任何此类争端或索赔的裁决。如果您是在欧盟有惯常居所的消费者，您还可以提出索赔，以在专属管辖地或您居住的欧盟国家执行您的消费者权利。此外，您还可以使用在线争议解决平台，可通过以下网址访问：https://ec.europa.eu/consumers/odr/。但在正式提出任何索赔之前，请考虑先与我们联系。

如果这些条款的各语言版本之间出现任何差异，则始终以此处提供的英文版本为准。

通用条款

ESET 保留随时通过更新相关文档来反映法律更改或帐户更改，从而修订这些条款和文档或其中任何部分的权利。系统将通过帐户通知您这些条款的修订。如果您不同意这些条款的更改，您可以注销您的帐户。除非您在收到有关这些更改的通知之前注销您的帐户，否则您将受这些条款的任何修正或修订的约束。请定期访问此页面以查看适用于帐户使用的当前条款。

通知

所有通知必须交付给: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic

附件 1

最终用户许可协议 for ESET Inspect Connector

附件 2

数据处理协议

附件 3

标准合同条款

最终用户许可协议 for ESET INSPECT Connector

自 2024 年 1 月 31 日开始有效

重要说明:在下载、安装、复制或使用前，请仔细阅读产品应用程序的以下条款。**下载、安装、复制或使用本软件即表示您同意这些条款和条件并承认隐私政策** 隐私政策

最终用户许可协议

本最终用户使用许可协议(“协议”)由 ESET, spol. s r. o..(“ESET”或“提供商”)与作为自然人或法人的您(“您”或“最终用户”)签订ESET 位于 Einsteinova 24, 85101 Bratislava, Slovak RepublicBIN 31333532协议授权您使用此处条款 1 中定义的软件。此处条款 1 中定义的软件可能存储在数据承载工具上、通过电子邮件发送、从 Internet 下载、从提供商的服务器下载或者按照以下指定的条款从其他来源获得。

这不是购买合同，而是关于最终用户权利的协议。无论是此软件的副本，还是经过商业包装的包含此软件的物理介质，亦或根据本协议最终用户有权使用的任何其他副本，所有权均归提供商所有。

在安装、下载、复制或使用软件过程中单击“我接受”或“我接受…”，即表示您同意本协议的条款和条件并确认隐私政策。如果您不同意本协议的任意条款及条件和/或隐私政策，请立刻单击取消选项、取消安装或下载、销毁或退还本软件、安装介质、随附文档和购买发票给提供商或您从中获取软件的渠道。

您同意使用软件表示您已经阅读本协议，您理解并同意遵守本协议的条款。

1.**软件。**本协议中的“软件”是指: (i) 本协议附带的计算机程序及其所有组成部分(ii) 磁盘CD-ROMDVD电子邮件及任何附件或附带本协议提供的其他介质的所有内容，包括数据承载工具提供、通过电子邮件提供或通过 Internet 下载的对象代码形式的软件(iii) 任何有关本软件的书面说明材料和任何其他相关文档，包括但不限于所有软件说明、软件规格、软件特点或操作说明、使用软件的操作环境的说明、使用或安装软件的说明，或任何关于如何使用软件的说明(以下称“文档”)(iv) 软件的副本、软件错误的修复程序、软件的附加程序、软件的扩展、软件的修改版本及软件组件更新(如果有)，关于这一点，提供商根据本协议第 3 条授予您许可。软件将仅以可执行目标代码的形式提供。

2.**安装、计算机和许可证密钥。**数据承载工具上提供、通过电子邮件发送、从 Internet 下载、从提供商服务器下载或从其他来源获得的软件需要安装。文档中指定了安装方式。任何可能对本软件有不利影响的计算机程序或硬件都不能安装在安装本软件的计算机上。计算机是指硬件，包括但不限于个人计算机、笔记本电脑、工作站、掌上电脑、智能电话、手持电子设备或本软件针对其而设计并将于其上安装和/或使用的其他电子设备。任何可能对本软件有不利影响的计算机程序或硬件都不能安装在安装本软件的计算机上。计算机是指硬件，包括但不限于个人计算机、笔记本电脑、工作站、掌上电脑、智能电话、手持电子设备或本软件针对其而设计并将于其上安装和/或使用的其他电子设备。许可证密钥是指唯一的符号、字母、数字或特殊符号的序列，提供给最终用户以允许本软件的合法使用、其特定版本或根据本协议延长许可证的期限。

3.**许可**。如果您同意本条件，同意本协议条款并且遵守此处规定的所有条款，提供商将授予您以下权利(“许可”):

a) **安装和使用。**您将具有在计算机硬盘或其他永久介质中安装软件以进行数据存储，在计算机系统内存中安装和存储软件，实施、存储和显示软件的非独占、不可转让的权利。

b) **许可数量规定。**软件的使用权利受最终用户数量约束。一位最终用户指(i) 在一个计算机系统上安装软

件；或 (ii) 如果许可约束范围为邮箱数量，则单个用户指的是通过邮件用户代理"MUA"接收电子邮件的计算机用户。如果 MUA 接受电子邮件，然后将其自动分发到多个用户，则最终用户数量应根据收到电子邮件的实际用户数量确定。如果邮件服务器执行邮件网关的功能，则最终用户数量应等于上述网关所服务的邮件服务器用户数量。如果未指定数量的电子邮件地址（例如通过别名）指向一个用户，用户接受这些地址，并且客户端不自动将邮件分发给大量用户，则需要一台计算机的许可证。您不得同时在多台计算机上使用同一许可。仅当最终用户根据限制（因提供商授予的许可证数量而引起）而有权使用本软件时，最终用户才有权输入本软件的许可证密钥。许可证密钥被视为保密信息，除非本协议或提供商允许，否则您不得与第三方共享许可证或允许第三方使用许可证密钥。如果您的许可证密钥被盗用，请立即通知提供商。

c) **家庭版/商业版。**本软件的家庭版应仅在私人和/或非商业环境中专供家庭和家人使用。必须获得本软件的商业版，才能在商业环境中使用，以及将本软件用于邮件服务器、邮件中继、邮件网关或 Internet 网关。

d) **许可条款。**您使用软件的权利将受时间限制。

e) **OEM 软件。**分类为"OEM"的软件应限于在您获得该软件的计算机上使用。不得转移到其他计算机。

f) **NFR/试用软件。**分类为"非转售性"NFR 或试用的软件不得用于付费用途，只能用于演示或测试软件功能。

g)**许可终止。**许可将在授予的期限结束时自动终止。如果不遵守本协议的任何条款，提供商有权撤销协议，不影响提供商在此类不测事件下的任何权利或合法补救措施。如果取消许可，您必须立刻删除、销毁本软件及所有备份副本，或自行承担费用将软件及所有备份副本返还至 ESET 或您购买软件的地方。在许可终止后，提供商有权取消最终用户使用本软件功能（这些功能需要连接到提供商的服务器或第三方服务器）的权利。

4.**具有数据收集和 Internet 连接要求的功能。**要正确操作本软件，需要连接到 Internet并且必须定期连接到提供商服务器或第三方服务器和遵循"隐私政策"的适用的数据收集。要正常使用本软件以及更新和升级本软件，必须连接 Internet 并收集适用数据。提供商有权发布本软件的更新或升级（即"更新"），但没有义务提供更新。此功能在软件标准设置下启用，因此自动安装更新，除非最终用户禁用自动安装更新。为了提供更新，需要进行许可证真实性验证，包括根据"隐私政策"获取其上安装本软件的计算机和/或平台的相关信息。

任何更新的提供可能都要遵循生命周期结束政策（即"EOL 政策"），可通过访问 https://go.eset.com/eol_business 了解该政策。在本软件或其任何功能达到 EOL 政策中定义的生命周期结束日期后，将不会提供任何更新。

就本协议而言，有必要收集、处理和存储数据，使提供商能够根据隐私政策识别您的身份。您特此承认提供商以自有方式检查您是否按照本协议条款使用此软件。您特此承认，就本协议而言，需要通过与提供商计算机系统或作为其分销和支持网络的商业合作伙伴进行软件通信来传输数据，以确保软件功能正常、授权使用软件以及保护提供商的权利。

本协议缔结后，提供商或作为其分销和支持网络的任何商业合作伙伴均有权传输、处理和存储标识您的重要数据，用于计费目的、本协议的履行以及您计算机上通知的传输。

关于隐私、个人数据保护和您作为数据主体所拥有权利的详细信息可以在"隐私政策"（"隐私政策"可在提供商的网站上找到，并可在安装过程中直接访问）中找到。您还可以从软件的帮助部分中访问此信息。

5.**行使最终用户的权利**。您必须亲自或通过员工行使最终用户权利。您只能将软件用于确保操作安全和保护购买了许可证的计算机或计算机系统

6.**权利的限制。**您不得复制、分发、提取组件或创建软件的衍生版本。使用软件时，您必须遵守以下限制：

a) 您可以在永久存储介质上创建一份软件副本作为备份副本，前提是不在任何其他计算机上安装或使用该存档备份副本。创建软件的任何其他副本应视为违反本协议。

b) 您不得以本协议明确提供的方式以外的任何其他方式使用、修改、翻译、复制或转让软件或软件副本的使用权。

c)您不得出售软件、授予从属许可、将软件出租给他人，或从他人租用软件或借出软件用于提供商业服务。

d) 您不得在法律明确禁止此类限制的范围之外以任何其他方式反向工程、反编译、反汇编软件，或试图获得软件的源代码。

e) 您同意使用软件的方式必须符合有关软件使用的相关法律中的所有适用法规，包括但不局限于，符合版权法和其他知识产权中适用的限制。

f) 您同意将只以不会限制其他最终用户获取这些服务的可能性的方式使用该软件及其功能。提供商保留限制向个体最终用户提供的服务范围，以确保最大数量的最终用户能够使用服务的权利。限制服务范围还将意味着完全杜绝在提供商的服务器或与软件的特定功能相关的第三方服务器上使用软件的任何功能和删除数据及信息的可能性。

g) 您同意不从事涉及使用许可证密钥的任何违反本协议条款的活动，或向任何无权使用本软件的人员提供许可证密钥，例如以任何形式转让已使用或未使用的许可证密钥，以及未经授权复制或分发复制或生成的许可证密钥，或从提供商以外的来源获得许可证密钥从而使用本软件。

7.**版权**。软件及所有权利，包括但不局限于所有权和知识产权，归 ESET 和/或其许可提供商所有。它们受国际条约条款以及使用此软件的国家的所有其他适用法律保护。软件的结构、组织和代码均为 ESET 和/或其许可提供商的重要商业机密和保密信息。您不得复制软件，第 6 (a) 款中指定的情况除外。允许按照本协议创建的任何副本必须包含与软件上显示的相同版权和其他所有权声明。如果您反向工程、反编译、反汇编源或试图以违反本协议条款的方式获得软件源代码，则您同意自此类行为开始起获得的任何信息将自动且不可逆地转让给提供商，并全部为提供商所有。

8.**保留权利**。除本协议中未明确授予您作为软件最终用户的权利以外，提供商特此保留所有软件权利。

9.**多个语言版本，双介质软件，多个副本**。如果软件支持多个平台或多种语言，或者如果您获得多个软件副本，则只能将软件用于已购买许可的计算机系统数量和版本。您不得将不使用的软件的任何版本或副本出售、出租、租用、授予从属许可、借出或转让给其他人。

10.**协议开始和终止。**本协议自您同意本协议条款之日起生效。您可以通过永久卸载、销毁或返还（费用自付）软件、所有备份副本以及提供商或其商业合作伙伴提供的所有相关材料来随时终止本协议。您使用软件及其任何功能的权利可能要遵循 EOL 政策。在本软件或其任何功能达到 EOL 政策中定义的生命周期结束日期后，您使用本软件的权利将终止。不考虑本协议终止方式，第 7、8、11、13、19 和 21 款的条款应保持无限期有效。

11.**最终用户声明**。作为最终用户，您了解软件“按原样”提供，不带任何明示或暗示担保，在适用法律允许的最大范围内。提供商、其许可提供商或分支机构或者版权所有者都不得提供任何明示或暗示的陈述或保证，包括但不限于适销性保证、特定用途适用性保证或对软件不侵犯任何第三方专利、版权、商标或其他权利的保证。提供商或任何其他方均不保证软件包含的功能符合您的要求，或软件操作将顺畅无错为实现预期目的而选择此软件以及安装、使用此软件和软件应用结果的全部责任和风险由您承担。

12.**无其他义务**。除本协议特别列出的义务以外，本协议不对提供商及其许可提供商施加任何其他义务。

13.**责任限制**。在适用法律允许的最大范围内，任何情况下提供商、其员工或许可提供商均不对以下损失负责：在适用法律允许的最大范围内，任何情况下提供商、其员工或许可提供商均不对以下损失负责：以任何形式造成的任何赢利、收入或销售额损失，任何数据损失，为获得备用物品或服务支付的额外费用，财产损失、人身伤害，营业中断，商业信息损失，或任何特殊、直接、间接、意外、经济、涵盖、犯罪、特殊或后继损失。无论这些损失是由合约、故意误操作、疏忽或其他责任理论造成，还是因安装、使用或无法使用本软件导致，提供商、其员工或许可提供商均不负责，即使已经通知提供商或其许可提供商或分支机构此类损失的可能。由于某些国家和某些法律不允许免责，但可能允许责任限制，因此提供商、其员工或许可提供商的责任应限制为您购买许可所支付的价格。

14. 本协议中的任何条款均不影响被法律认可具备消费者权利和地位的一方的权利。

15.**技术支持**ESET 或 ESET 委托的第三方将出于自行考量提供技术支持，不具有任何保证或声明。在本软件或其任何功能达到EOL政策中定义的生命周期结束日期后，将不会提供任何技术支持。提供技术支持前，最终用户需要备份所有现有数据、软件和程序工具ESET 和/或 ESET 委托的第三方不承担因提供技术支持导致的数据、财产、软件或硬件破坏或损失或者利润损失ESET 和/或 ESET 委托的第三方保留决定解决问题是否超出技术支持范围的权利ESET 保留出于自行考量拒绝、暂停或终止提供技术支持的权利。出于提供技术支持的目的，可能需要遵循“隐私政策”的许可证信息、信息和其他数据。

16.**转让许可**。除非违背协议条款，否则软件可以在不同计算机系统之间转移。如果不违背协议条款，最终用户仅有权在提供商同意下，将许可及从本协议产生的所有权利转让给其他最终用户，并受以下条款约束(i) 原始最终用户不得保留软件的任何副本(ii) 权利转让必须从原始最终用户转交给新最终用户(iii) 新最终用户必须承担原始最终用户在本协议条款下承担的所有权利和义务(iv) 原始最终用户必须向新最终用户提供文档，证明第 17 款下指定的软件正版性。

17.**证明软件的正版性。**最终用户可以采用以下任意方式证明软件的使用权(i) 通过提供商或提供商指定的第三方发布的许可证书(ii) 通过书面许可协议，如果已缔结此类协议(iii) 通过提交发送给提供商的包含许可详细信息(用户名和密码)的电子邮件。出于证明软件正版性的目的，可能需要遵循“隐私政策”的许可证信息和最终用户身份数据。

18.**政府当局和美国政府许可**。软件提供给政府当局（包括美国政府）时具有本协议介绍的许可权利和限制。

19.**贸易控制合规性**

a) 您将不得直接或间接地向任何人出口、再出口、转让或以其他方式提供该软件，不得以任何方式使用该软件，也不得涉及任何行为，否则可能导致 ESET 或其控股公司、其子公司及其任何控股公司的子公司以及由其控股公司控制的实体（“关联公司”）违反《贸易管制法》或承担《贸易管制法》所规定的不良后果，包括

i. 美国、新加坡、英国、欧盟或其任何成员国的任何政府、州或监管机构、将履行本协议规定义务的国家/地区、成立或运维 ESET或其任何关联企业的国家/地区颁布或通过的针对出口、再出口或转让商品、软件、技术或服务进行控制、限制或施加许可要求的任何法律，和

ii. 美国、新加坡、英国、欧盟或其任何成员国的任何政府、州或监管机构、将履行本协议规定义务的国家/地区、成立或运维ESET或其任何关联企业的国家/地区实施的任何经济、金融、贸易或其他方式的制裁、限制、禁运、进出口禁令、禁止转移资金或资产或提供服务或其他等效措施。

（上述“i.”和“ii.”部分中提到的法律行为统称为“《贸易管制法》”）。

b) 如果发生以下情况ESET 有权立即中止或终止这些条款所规定的义务：

i.ESET 合理认为用户已违反或可能违反了本协议第 19 a) 款的规定；或

ii. 最终用户和/或软件受《贸易管制法》约束，因此 ESET 合理认为继续履行本协议所规定的义务可能会导致 ESET 或其关联公司违反《贸易管制法》，或承担《贸易管制法》所规定的不良后果。

c) 本协议无意，也不应理解或解释为诱导或要求任何一方以不遵循《贸易管制法》、受《贸易管制法》处罚或禁止的方式行事或不作为（或者同意行事或不作为）。

20.**通知**。所有通知、返还的软件和文档必须交付给ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic但不影响 ESET 根据本协议的第 22 条有权向您传达对本协议、隐私政策EOL 政策以及文档所做的任何更改ESET 可能会通过软件向您发送电子邮件、应用内通知，也可能会在我们的网站上发布通信帖子。您同意接收 ESET 以电子形式发送的法律通信，包括有关条款、特殊条款或隐私政策变更的任何通信、任何合同修改/赞同、要约邀请、通知或其他法律通信。此类电子通信应等同于书面形式接收，除非适用

法律明确要求采用其他形式的通信。

21.**适用法律**。本协议受斯洛伐克法律管辖，并按斯洛伐克法律解释。最终用户和提供商同意，法律与联合国国际货物销售合同公约之间的冲突原理不适用。您明确同意，与提供商之间发生的任何索赔或争端，或任何方式的与软件使用相关的索赔或争端，其唯一裁决权属于斯洛伐克布拉迪斯拉发第一地区法院，并且您明确同意上述法院作出的裁决。

22.**通用条款**。如果本协议中的任何条款无效或无法执行，将不影响协议其他条款的有效性，按照此处规定的条款这些条款仍然有效且可执行。本协议已以英文履行。如果出于方便目的或任何其他目的而准备了本协议的任何翻译，或者本协议的各语言版本之间存在差异，则以英文版本为准。

ESET 保留随时更改本软件以及出于以下目的修订本协议的条款、其附件、附录、隐私政策、EOL 政策和文档或其任何部分的权利：(i) 反映对本软件或 ESET 开展业务方式的更改；(ii) 出于法律、法规或安全原因，或 (iii) 防止滥用或损害。将通过电子邮件、应用内通知或其他电子方式通知您本协议的任何修订。如果您不同意对本协议的拟议变更，可以在收到变更通知后的 30 内，根据第 10 条终止履行本协议。除非您在该时限内终止履行本协议，否则拟议变更将视为被接受，并自您收到变更通知之日起开始对您生效。

您与提供商签署的本协议是关于本软件的唯一完整协议，它完全取代任何之前的关于软件的表述、讨论、承诺、沟通或广告。

EULAID: EULA-PRODUCT-LG-EI; 3537.0

协议附录

将信息转发给提供商。适用于“将信息转发给提供商”的附加条款如下所示：

本软件包含多项功能，这些功能用于收集计算机病毒和其他恶意计算机程序与可疑对象、问题对象、潜在不受欢迎对象或潜在不安全对象（例如文件、URL、IP 数据包和以太网帧）的样本（以下简称“渗透”）并将其发送给提供商，包括但不限于安装过程、安装本软件的计算机和/或平台的信息和/或本软件的操作和功能信息（以下简称“信息”）。这些信息和渗透可能包含已安装本软件的计算机上的最终用户或其他用户的数据（包括随机或意外获得的个人数据），以及受附带相关联元数据的渗透影响的文件。

LiveGrid 信誉系统功能可以收集这些信息和渗透，包括将与渗透有关的单向哈希收集起来并发送给提供商。可在本软件的标准设置下启用此功能。

提供商将仅使用获得用于分析和研究渗透以及改善软件和许可证真实性验证的信息和渗透，并将采取合理措施确保收到的渗透和信息安全。通过激活软件的此功能，即表示您同意将渗透和信息发送给提供商，并且您还准许提供商根据相关法律规定获得必要批准，以处理所获渗透和信息。您可以随时停用此功能。

EULAID: EULA-PRODUCT-LG-EI; 3537.0

数据处理协议

根据欧洲议会和理事会于 2016 年 4 月 27 日就保护自然人在个人数据处理和此类数据自由移动方面作出的规定 (EU) 2016/679 的要求，废除指令 95/46/EC（以下简称“GDPR”）向提供商（以下简称“处理者”）与您（以下简称“控制者”）订立数据处理合同关系，以便规定个人数据处理的条款和条件、个人数据保护方式，以及规定在将本条款的内容作为主合同履行的过程中双方在处理数据主体（代表控制者）的个人数据时的其他权利和义务。

1.**个人数据处理。**依据这些条款提供的服务包括处理隐私政策中列出的已识别或可识别自然人的相关信息（以下简称“个人数据”）。

2.**授权。**控制者授权处理者处理个人数据，包括以下说明：

(i) “处理目的”是指根据本条款提供服务，处理者仅被允许代表控制者依据控制者所要求的服务条款处理个人数据。出于其他目的所收集的全部信息在控制者-处理者合同关系之外进行处理。

(ii) 处理周期是指按照本条款确立相互合作至终止服务为止的一段时间，

(iii) 个人数据的范围和类别。这些服务仅会处理一般个人数据。但是，控制者全权负责确定个人数据范围。

(iv) “数据主体”是指自然人作为控制者的设备的授权用户，

(v) 处理活动是指出于处理目的而所需执行的一切和所有操作，

(vi) “记载说明”是指本条款、其附件、隐私政策和服务文档中所述的说明。控制者应对处理者依据数据保护法的相应适用条款处理个人数据的法律许可负责。

3.**处理者的义务**。处理者负责以下事项：

(i) 仅根据书面说明以及出于条款、其附件、隐私政策和服务文档中定义的目的处理个人数据，

(ii) 根据 GDPR 向获授权处理个人数据的人员（以下简称“获授权人员”）指示其权利和义务以及他们的违规责任，并确保获授权人员承诺保密并按照书面说明操作，

(iii) 实施并遵循条款、其附件、隐私政策和服务文档中所述的措施，

(iv) 协助控制者应对数据主体涉及其权限的请求。未经控制者的指示，处理者不得更正、删除或限制个人数据的处理。代表控制者处理的数据主体就其个人数据的所有请求应立即转发给控制者。

(v) 协助控制者向监管机构和数据主体通知个人数据泄露，处理者应在发现任何违反个人数据处理或个人数据安全的行为后立即通知控制者。处理者应在合理范围内协助调查并消除此类违规行为，并采取合理措施来进一步限制不良影响。

(vi) 根据控制者的选择，可在处理期结束后将所有个人数据删除或返还给控制者。控制者承诺在处理期结束后十（10）天内将其决定告知处理者。该规定不得影响处理者出于公共利益、科学研究目的、统计目的或为确立、行使或辩护合法要求的目的而有必要保留个人数据的权利。

(vii) 确保代表控制者执行的所有类别处理活动的记录保持最新，

(viii) 使证明合规性所需的全部信息能够作为条款、其附件、隐私政策和服务文档的一部分提供给控制者。如果控制者方对个人数据处理进行审核或控制，则控制者有义务在计划审核或控制前至少三十（30）天以书面形式通知处理者。

4.**雇佣其他处理者。**处理者有权雇佣其他处理者来执行特定的处理活动，例如依据条款、其附件、隐私政策和服务文档来为服务提供云存储和基础设施。当前Microsoft 提供的云存储和基础设施作为 Azure 云服务的一部分。即使在这情况下，处理者应仍是唯一的联络点，并且是对合规性负责的一方。处理者特此承诺，在出于可能反对此类改变目的而添加或替换其他处理者时会告知控制者。

5.**处理的地域。**处理者确保执行处理的所在地位于欧洲经济区或欧洲委员会根据控制者的决定确认为安全的国家/地区。如果传输和处理所在地位于欧洲经济区或欧洲委员会根据控制者的请求经决定确认为安全的国家/地区之外，则应适用标准合同条款。

6.**安全性。**处理者通过了 ISO 27001:2013 认证，并且在对网络层、操作系统、数据库、应用程序、人员和操作流程应用安全控制时使用 ISO 27001 框架来实施分层防御安全策略。定期评估和审查是否符合法规和合同要求（对处理者的其他基础设施和操作执行类似评估和审查），并采取必要步骤以持续确保合规性。处理者已使用基于 ISO 27001 的 ISMS 来组织数据安全性。安全文档主要包括信息安全、物理安全以及设备安全性、事件管理、处理数据泄露和安全事件等的策略文档。

7.**技术和组织措施**。处理者应保护个人数据，以免遭偶然和非法的损坏和破坏、偶然丢失、更改、未经授权的访问和披露。为此，处理者应按照 GDPR 的要求，为保护数据主体的权利而针对处理模式和处理所带来的风险采取适当技术和组织措施。在安全策略中，详细说明了技术和组织措施。

8.**处理者的联系信息。**有关个人数据保护的所有通知、请求、需求和其他通信应寄送给 ESET, spol. s.r.o.正式地址如下Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: dpo@eset.sk

标准合同条款

SECTION I

Clause 1 Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter

and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to

becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation (2) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the

latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (3) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and

organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter (5).

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in

Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate

its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (6) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set

out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data (7), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9 Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (9) The Parties agree that, by complying with this Clause, the data importer fulfils its

obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. (10) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a

representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition,

with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law as defined in Terms.

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law as defined in Terms.

Clause 18 Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts as defined in Terms.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts as defined in Terms.

APPENDIX

EXPLANATORY NOTE: It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Controller as defined in Data Processing Agreement

2. Processor as defined in Data Processing Agreement

(based on the flow of data)

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1. Controller as defined in Data Processing Agreement

2. Processor as defined in Data Processing Agreement

(based on the flow of data)

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred: As defined in Data Processing Agreement.

Categories of personal data transferred: As defined in Data Processing Agreement and Privacy Policy.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: As defined in Data Processing Agreement and Privacy Policy.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous basis.

Nature of the processing: Automated.

Purpose(s) of the data transfer and further processing: Provision of service as defined in Terms, its Annexes, Privacy Policy, and service documentation.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: As defined in Data Processing Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: As defined in Data Processing Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13: As defined in Privacy Policy

ANNEX II TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons: As defined in Security

Policy

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors: As defined in Data Processing Agreement

References:

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(2) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(3) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(4) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(5) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

(6) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not

qualify as an onward transfer for the purposes of these Clauses.

(7) This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

(8) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(9) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(10) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(11) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(12) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

隐私政策

自 2022 年 3 月 23 日起生效

保护个人数据对作为数据控制者的 ESET, spol. s r. o.□注册办公室位于 Einsteinova 24, 851 01 Bratislava, Slovak Republic□业务识别号：31333532，以下简称"ESET"或"我们"）而言尤为重要。我们希望遵守依据《欧盟一般数据保护条例□□"GDPR"□作为法律上所规定的透明度要求。为了达到上述目的，我们发布此隐私政策，唯一目的是告知我们的客户（即作为数据主体的"最终用户"或"您"）有关以下个人数据保护主题的信息：

- 个人数据处理的法律依据、
- 数据共享和机密性、
- 数据安全性、
- 作为数据主体的权利、
- 个人数据的处理
- 联系人信息。

个人数据处理的法律依据

在数据处理方面，我们根据与个人数据保护有关的适用法律框架所用到的法律依据较少ESET 处理个人数据主要是为了履行 使用条款 （“条款”）（针对最终用户GDPR 第 6 (1) (b) 款），这适用于提供 ESET 产品或服务，除非另有明确说明，例如：

- 合法权益法律依据GDPR 第 6 (1) (f) 款），使我们可以处理有关客户如何使用我们的服务及其满意度的数据，从而为用户提供我们所能提供的最佳保护、支持和体验。甚至营销也被适用法律确认为合法权益，因此我们通常据此与客户沟通营销。
- 同意GDPR 第 6 (1) (a) 款），当我们认为此法律依据是最适合的法律依据或法律所要求时，我们可能会在特定情形下向您提出要求。
- 遵守法律义务GDPR 第 6 (1) (c) 款），例如订立电子通信、发票或账单文件保留的要求。

数据共享和机密性

我们不会与第三方共享您的数据。但是ESET 是一家通过附属公司或合作伙伴（作为我们销售、服务和支持网络的一部分）在全球运营的公司。出于履行最终用户许可协议的目的（例如，提供服务或支持ESET 所处理的许可、计费和技术支持信息可能会在附属公司或合作伙伴之间传输。

ESET 更愿意在欧盟 (EU) 内处理其数据。但是，根据您所在的位置（在欧盟以外使用我们的产品和/或服务）和/或您选择的服务，可能需要将您的数据传输到欧盟以外的国家/地区。例如，我们使用与云计算相关的第三方服务。在这些情况下，我们会仔细选择服务提供商，并确保通过合同以及技术和组织措施提供相应级别的数据保护。通常，我们同意欧盟标准合同条款，并在必要时提供补充合同规定。

对于欧盟以外的一些国家/地区（例如，英国和瑞士），欧盟已确定提供同等级别的数据保护。由于提供同等级别的数据保护，因此向这些国家/地区传输数据不需要任何特殊授权或协议。

我们依赖第三方服务并与外部处理者合作，来提供与云计算、计费等相关的服务。

数据安全性

ESET 会实施适当技术和组织措施来确保与潜在风险相称的安全级别。我们会尽最大努力来确保处理系统和服务的持续机密性、完整性、可用性和弹性。但当发生导致您的权利和自由遭受威胁的数据泄漏时，我们会随时通知相关监管机构以及作为数据主体的受影响最终用户。

数据主体的权利

每个最终用户的权利都很重要，我们会告知您，所有最终用户（来自任何欧盟或任何非欧盟国家/地区）在 ESET 都享有以下权利。要行使您数据主体的权利，可以通过支持表单或发送电子邮件至 dpo@eset.sk 与我们联系。出于识别目的，我们会要求您提供以下信息：姓名、电子邮件地址以及（如果有）许可证密钥或客户编号和公司隶属关系。请勿向我们发送任何其他个人数据，例如出生日期。我们想指出的是，为了能够处理您的请求以及出于识别目的，我们将处理您的个人数据。

撤消同意的权利。撤消同意的权利仅适用于基于同意进行处理的情况。如果我们根据您的同意处理您的个人数据，则您有权随时撤消同意，而无需给出理由。撤消您的同意仅对将来处理有效，并不影响撤消之前所处理数据的合法性。

反对权。反对处理的权利适用于基于 ESET 或第三方合法权益的处理。如果我们处理您的个人数据是为了保护合法权益，则您作为数据主体有权随时反对我们所谓的合法权益和对您个人数据的处理。您的反对仅对将来处理有效，并不影响反对之前所处理数据的合法性。如果我们出于直接营销目的处理您的个人数据，则无需给出您的反对理由。这也适用于资料收集，因为它与此类直接营销有关。在所有其他情况下，我们要求您简要告知我们针对 ESET 处理您个人数据的合法权益提出的投诉。

请注意，在某些情况下，尽管您撤消了同意，但我们有权根据其他法律依据进一步处理您的个人数据（例

如，为了履行合同）。

访问权。您作为数据主体，有权随时免费获取有关 ESET 存储您数据的信息。

纠正权。如果我们无意中处理了有关您的错误个人数据，您有权更正该数据。

删除权和限制处理权。您作为数据主体，有权要求删除或限制处理您的个人数据。如果我们处理您的个人数据（例如，在您同意的情况下），而您撤消同意并且没有其他法律依据（例如，合同），则我们会立即删除您的个人数据。在我们的保留期结束时，如果不再需要您的个人数据用于为其规定的目的，您的个人数据也会被删除。

如果我们将您的个人数据用于直接营销的唯一目的，而您已撤消同意或反对 ESET 的潜在合法权益，则我们将限制对您个人数据的处理，以便将您的联系方式数据包括在我们的内部黑名单中，从而避免主动联系。否则，将删除您的个人数据。

请注意，我们可能需要存储您的数据，直到立法者或监管机构发布的保留义务和期限到期。保留义务和期限也可能源于斯洛伐克法律。其后，将例行删除相应的数据。

数据迁移。我们很乐意为您（作为数据主体）提供 ESET 采用 xls 格式处理的个人数据。

提出投诉的权利。您作为数据主体，有权随时向监管机构提出投诉。ESET 遵守斯洛伐克法律的规定，并且我们受欧盟的数据保护法的约束。相关数据监管机构是斯洛伐克共和国个人数据保护办公室，具体地址为 Hraničná 12, 82007 Bratislava 27, Slovak Republic。

个人数据的处理

由 ESET 提供并在我们基于 Web 的产品中实现的服务都是根据使用条款（“ToU”）进行提供，但其中一些服务可能需要特别关注。我们希望为您提供与产品和服务提供有关的数据处理的更多详细信息。我们提供以下各项中所述的各种服务： 的 ESET Password Manager 的条款 和产品 文档处理从您或您的产品收集的数据，其中一些数据可能包含个人数据。为了正常运行，我们需要收集以下信息：

ESET 充当处理者

- **受监视的端点设备和网络**：ESET Inspect Cloud 收集并处理来自受监视的端点设备和网络的数据，并将其发送到云控制台。由于该产品是一种用于详细监视和异常检测的端点检测和响应 (EDR) 产品类型，因此该产品会在已部署它的端点上收集以下相关信息：活动和操作系统事件（包括有关在计算机上找到的所有可执行模块的信息）、低级别事件（如进程创建、文件修改、注册表修改、网络连接）和所有发现的威胁（恶意软件、PUA、被阻止的网页等）。请注意，处理后的数据可能包含隐私敏感信息，如所有已修改文件的名称、所有进程的命令行以及所有受访页面的 URL。
- ESET Inspect Cloud 包含某些预定义的监视规则，但在您的基础架构中实际执行的监视范围以及收集的确切数据取决于您和您的管理员管理的规则、排除项和设置。因此，我们将根据本条款中包含的《数据处理协议》以您的数据处理者的身份处理此类数据，仅向您提供我们的服务。我们将按照我们的《日志保留政策》，在有限时间段内存储这些数据。
- 我们鼓励您在设置 ESET Inspect Cloud 时检查和查看您所在国家/地区有关数据收集和处理的立法和法律要求。您可能需要向用户告知受监视的端点设备，或请求特定管辖范围内的特定权限以执行监视活动。

ESET 充当控制者

- **许可和计费数据**：ESET 会收集和处理姓名、电子邮件地址、许可证密钥以及（如果适用）地址、公司隶属关系和付款数据，以方便许可证激活、许可证密钥交付、到期提醒、支持请求、许可证真实性验证、提供我们的服务和其他通知（包括依据适用法律或在您同意的情况下发送营销邮件）。ESET 有法律义务将计费信息保留 10 年，但许可信息将在许可证到期后的 12 个月之内进行匿名化处理。

- **产品正常运行所需的数据**。其他处理的信息可能包括：安装过程相关信息（包括安装产品的平台）以及我们产品或托管设备的操作和功能信息，例如产品的硬件指纹、安装 ID、许可证 ID、IP 地址、MAC 地址、使用的电子邮件地址或配置设置。
- **统计数据和遥测数据**。为了增强我们基础架构的安全性、维护和改进我们的服务，需要处理有关服务使用情况的遥测信息。我们仅对这些信息进行汇总处理，包括数据库性能、运行状况统计信息、托管端点数量、端点系统操作系统、系统硬件、系统错误、策略、登录、任务、通知、托管设备、检测统计信息、事件处理率、规则引擎统计信息、排除项等数据以及 HTTP 标头。
- **技术支持**。支持服务可能需要在您的支持请求中包含联系方式和许可信息及数据。根据您选择与我们联系的渠道，我们可能会收集您的电子邮件地址、电话号码、许可证信息、产品详细信息和支持案例的描述。为了便于提供支持服务，可能会要求您提供给我们其他信息。为技术支持而处理的数据存储 4 年。

请注意，如果使用我们产品和服务的用户不是已购买产品或服务并与我们签订条款的最终用户（例如，最终用户的雇员、家庭成员或最终用户依据条款向其授权使用产品或服务的用户），则 ESET 依据 GDPR 第 6 (1) (f) 款规定的合法权益执行数据处理，以使最终用户授权的用户能够使用我们依据条款提供的产品和服务。

联系人信息

如果您希望行使作为数据主体的权利或有疑问，请发送邮件至：

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk