Annex
Technical and Organisational Security Measures

I Purpose of processing, categories of data involved, categories of affected data subjects

1. Categories of data subjects
Employees and other participants - individuals of the Corporate User's Peero community

2. Type of personal data

(a) Categories of personal data
Name, surname, e-mail address, position held, department within the company, country of location/ corporate adherence country of the data subject

The Corporate User at its discretion may add to the particular Peero community individuals belonging to group of companies/ organizations the Corporate User represents or is part of

(b) Special categories of personal data

Are not processed

3. Nature of the processing
Providing a feedback service (assessment and feedback) through the Peero App to the Corporate User as Controller and indirectly to data subjects - individuals added to the Peero community of the Corporate User

4. Length of processing

Until accomplishment of each individual task of the Corporate User, subject to the term of validity of the Agreement

II Technical and organizational measures

1. Physical Access Control
Physical access is controlled according to rules of the manufacturer of the resource used - Microsoft Azure (https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security)
It shall include at least, but not limited to:
- Providing physical protection for the technological resources on which data are processed
- Restriction of access to data
- Access control key management
- Choice of appropriate staff, service personnel
- Provision of monitoring equipment
- Providing virtually separate data processing equipment

Pielikums
Tehniskie un organizatoriskie drošības pasākumi

I Apstrādes mērķis, iesaistītās datu kategorijas, ietekmēto datu subjektu kategorijas

1. Datu subjektu kategorijas
Darbinieki un citi Korporatīvā lietotāja Peero kopienas dalībnieki - fiziskās personas

2. Personas datu veidi

(a) Personas datu kategorijas
Datu subjekta vārds, uzvārds, e-pasta adrese, amats uzņēmumā, uzņēmuma departaments, atrašanās vietas/ korporatīvās piederības valsts

Korporatīvais lietotājs pēc saviem ieskatiem var pievienot konkrētai Peero kopienai fiziskās personas, kuras pieder uzņēmumu/organizāciju grupai, kuras Korporatīvais lietotājs pārstāv vai ir to daļa

(b) Īpašās personu datu kategorijas

Netiek apstrādātas

3. Apstrādes veids
Ar Peero lietotnes starpniecību atgriezeniskās saites pakalpojuma (novērtējuma un atsauksmes) sniegšana Korporatīvajam lietotājam kā Pārzinim un pastarpināti Korporatīvā lietotāja Peero kopienai piesaistītajiem datu subjektiem

4. Apstrādes ilgums

Līdz katra atsevišķa Korporatīvā lietotāja darba uzdevuma izpildei, ievērojot Līguma spēkā esamības termiņu

II Tehniskie un organizatoriskie drošības pasākumi

1. Fiziskās pieejas kontrole
Tiek nodrošināta fiziskās pieejas kontrole atbilstoši izmantotā resursa - Microsoft Azure ražotāja noteikumiem (https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security).
Tas ietver vismaz, bet ne tikai:
- Fiziskās aizsardzības tehnoloģiskajiem resursiem, uz kuriem tiek apstrādāti dati, nodrošināšanu
- Pieejas tiesību datiem ierobežošanu
- Pieejas kontroles atslēgu pārvaldību
- Atbilstošu darbinieku, apkalpojošā personāla izvēli
- Uzraudzības iekārtu nodrošināšanu
- Virtuāli nodalītu datu apstrādes iekārtu nodrošināšanu

Приложение
Технические и организационные защитные меры

I Цель обработки, категории вовлеченных данных, категории затронутых субъектов данных

1. Категории субъектов данных
Работники и другие участники сообщества Peero Корпоративного пользователя - физические лица

2. Виды персональных данных

(а) Категории персональных данных
Имя, фамилия, адрес электронной почты, должность в компании, департамент предприятия, страна местоположения / страна корпоративной принадлежности субъекта данных

Корпоративный пользователь по своему усмотрению может добавить в конкретное сообщество Peero физические лица, принадлежащие группе предприятий/организаций, которых представляет Корпоративный пользователь или является их частью

(б) Специальные категории персональных данных

Не обрабатываются

3. Вид обработки
Предоставление услуг приложения Peero - обратная связь (оценка и отзывы) - для Корпоративного пользователя как Контролёра и опосредствованно субъектам данных привлеченным сообществу Peero Корпоративного пользователя

4. Продолжительность обработки

До выполнения каждого отдельного задания Корпоративного пользователя принимая во внимание срок действительности Договора

II Технические и организационные защитные меры

1. Контроль физического доступа
Обеспечивается контроль физического доступа в соответствии с правилами используемого ресурса изготовителя - Microsoft Azure (https://docs.microsoft.com/en-us/azure/security/chysical-security).
Оно включает по меньшей мере, но не только:
- Для технологических ресурсов физической защиты, на которые обрабатываются данные, обеспечение
- Ограничение прав доступа к данным
- Управление ключами контроля доступа
- Соответствующий выбор персонала, обслуживающего персонала
- Обеспечение надзорного оборудования

		· Обеспечение виртуально отдельного оборудования для обработки данных
2. Logical Access Control Access to the Peero App resources in Microsoft Azure is granted according to the "least permissive" principle and includes at least the following security aspects: · Multi-factor authentication requirements · Defining password security level · Auto-lock your computer · Authentication journaling details etc. The solutions applied by the Processor are described in detail in the internal corporate policies of the Processor	**2. Loģiskās pieejas kontrole** Pieeja Peero lietotnes resursiem Microsoft Azure tiek piešķirta pēc "least permissive" principa, un ietver ne mazāk kā šādus drošības aspektus: · Multi-faktoru autentifikācijas prasības · Paroles drošības līmeņa definējums · Datora automātiska bloķēšana · Autentifikācijas žurnalēšanas dati utml. Apstrādātāja piemērotie risinājumi ir detalizēti aprakstīti Apstrādātāja iekšējās korporatīvās politikās	**2. Управление логического доступа** Доступ к ресурсам приложения Peero в Microsoft Azure предоставляется по принципу «least permissive» и включает не менее следующих аспектов безопасности: · Требования многофакторной проверки подлинности · Определение уровня безопасности пароля · Автоблокировка компьютера · Данные журналов проверки аутентификации итд. Решения, примененные Обработчиком, подробно описаны в внутренних корпоративных политиках Обработчика
3. Data Access Control The Processor provides at least the following technical and organisational measures: · Development of internal rules and procedures (how data access is granted, changed, cancelled) · The process of granting and revoking access rights · Different access rights (e.g., defined roles) · Audit records · Disciplinary responsibility for employees accessing data without permission · Access reports (if there are audit records)	**3. Pieejas datiem kontrole** Apstrādātājs nodrošina ne mazāk kā šeit minētos tehniskos un organizatoriskos pasākumus: · Iekšējo noteikumu un procedūru izstrādi (kā tiek piešķirta, mainīta, anulēta pieeja datiem) · Pieejas tiesību piešķiršanas un anulēšanas procesu · Dažādas pieejas tiesības (piemēram, definētas lomas) · Auditācijas pierakstus · Disciplināratbildību darbiniekiem, kuri piekļūst datiem bez atļaujas · Ziņojumus par piekļuvi (ja ir auditācijas pieraksti)	**3. Контроль доступа к данным** Обработчик обеспечивает не менее упомянутых здесь технических и организационных мероприятий: · Разработка внутренних правил и процедур (как предоставляется, изменяется, аннулируется доступ к данным) · Процесс предоставления и аннулирования прав доступа · Разные права доступа (например, определенные роли) · Аудитационные записи · Дисциплинарное взыскание работников, которые без полномочий проник к данным · Сообщения о доступе (при наличии аудиторских записей)
4. Data loss prevention The Processor provides at least the following technical and organisational measures: · Isolated application infrastructure · Encryption when transmitting data (TLS minimum version 1.2, SSL) · Encryption for data storage facilities · Audit records · Backup copies · High availability of resources · Internet Application Firewall (WAF)	**4. Datu zuduma novēršana** Apstrādātājs nodrošina vismaz šādus tehniskos un organizatoriskos pasākumus: · Izolētu aplikācijas infrastruktūru · Šifrēšanu pārsūtot datus (TLS minimālā versija 1.2, SSL) · Šifrēšanu datu glabātuvēm · Auditācijas pierakstus · Rezerves kopijas · Augstu resursu pieejamību · Interneta Aplikāciju ugunsmūri (WAF)	**4. Предотвращение потери данных** Обработчик обеспечивает по меньшей мере следующие технические и организационные мероприятия: · Изолированная инфраструктура аппликации · Шифровка при пересылке данных (минимальная версия TLS 1.2, SSL) · Шифрование для хранилищ данных · Аудитационные записи · Резервные копии · Высокая доступность ресурсов · · Брандмауэр веб-приложений (WAF)
5. Segregation Control All representatives involved in the data processing by the Processor for maintenance of Peero App use single database, however the functions and access rights of data processors are segregated Processor is providing procedures in respect to storage, amendments to, deletion, transmitting of the data for different purposes	**5. Nodalīšanas kontrole** Visi Apstrādātāja datu apstrādē piesaistītie pārstāvji Peero lietotnes uzturēšanai izmanto vienotu datu bāzi, taču datu apstrādes veicēju funkcijas un pieejas tiesības ir nodalītas Apstrādātājs nodrošina procedūras datu glabāšanai, grozīšanai, dzēšanai, pārsūtīšanai dažādiem nolūkiem	**5. Контроль разделения** Все представители привлеченные Обработчиком в обработке данных, используют единую базу данных для поддержания приложения Peero, но функции и права доступа к данным, выполняющие обработку данных, разделены Обработчик обеспечивает процедуры для хранения, изменения, удаления, пересылки данных для различных целей
6. Integrity Audit records and generation of messages in systems to monitor activities therein - who has performed data entry, introduced changes or deleted data.	**6. Integritāte** Auditācijas pieraksti un ziņojumu ģenerēšana sistēmās, lai uzraudzītu darbības sistēmās - kurš ir veicis datu ievadīšanu, izmaiņas vai dzēšanu	**6. Целостность** Аудитационные записи и формирование отчетов в системах для отслеживания действий в них - кто ввел данные, внес изменения или удалил данные
7. Availability control Availability control is provided according to Microsoft Azure rules, implementation and compliance whereof is primarily monitored by Microsoft Corporation (https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-availability).	**7. Pieejamības kontrole** Pieejamības kontrole tiek nodrošināta atbilstoši Microsoft Azure noteikumiem, ko primāri pārrauga Microsoft Corporation (https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-availability). Tiek nodrošināti sekojoši tehniskie un organizatoriskie pasākumu:	**7. Контроль доступности** Контроль доступности осуществляется в соответствии с правилами Microsoft Azure, реализация и соблюдение которых в первую очередь контролируется корпорацией Microsoft (https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-availability).

The following technical and organisational measures are provided:
- Backup copies
- High accessibility

8. Performed tests of the system

A penetration testing was performed for the Peero App, which also included top 10 OWASP vulnerability exploits. This testing was performed by a certified person who did not participate in the product development.

III Approved Sub-Processors

A list of Approved Sub-Processors is available on site
PEERO DATA SUBPROCESSORS (EN)

Latest updates introduced in January 2023

- Rezerves kopijas
- Augsta pieejamība

8. Veiktie sistēmas testi

Peero lietotnei ir veikta ielaušanās testēšana, kurā tajā skaitā tika iekļauta top 10 OWASP ievainojamības pārbaudes. Šo testēšanu ir veikusi sertificēta persona, kura nepiedalījās produkta izstrādē.

III Apakšapstrādātāji

Apakšapstrādātāju saraksts ir pieejams vietnē
PEERO DATU APAKŠAPSTRĀDĀTĀJI (LV)

Pēdējo reizi pārskatīts 2023. gada janvārī

Обеспеченны следующие технические и организационные мероприятия:
- Резервные копии
- Высокая доступность

8. Проведенные тесты системы

Приложение Peero было подвергнуто тестированию на вторжение, которое также включало тест на уязвимость OWASP топ 10 эксплойтов. Это тестирование было выполнено сертифицированным лицом, не участвовавшим в разработке продукта.

III Субобработчики

Список субобработчиков доступен на веб-сайте
СУБОБРАБОТЧИКИ ДАННЫХ PEERO (RU)

Последнее обновление внесено в январе 2023 года