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, proof of task completion (images or links), delivery information, associated metadata.

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.

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, uzdevumu izpildes pierādījumi (attēli vai saites), piegādes dati, saistītie metadati.

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 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.

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.

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

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.

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
- u. tml.

Apstrādātāja piemērotie risinājumi ir detalizēti aprakstīti Apstrādātāja iekšējās korporatīvās politikās.

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

- Access reports (if there are audit records).

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)

5. Segregation Control

All representatives involved in data processing by the Processor for the maintenance of the Peero application use two databases: "Common Data" and "Application Data".

Common Data - A database that includes information related to authorization (including user data such as emails, encrypted passwords, and authorizations performed in the application).

Application Data - A database that includes information about actions performed in the application, settings, and users (including user data such as name, surname, email, country, department, and team).

6. Integrity

Audit records and generation of messages in systems to monitor activities therein - who has performed data entry, introduced changes, or deleted data.

7. Availability control

Availability control is provided according to Microsoft Azure rules, implementation and compliance whereof is primarily monitored by Microsoft Corporation

- Ziņojumus par piekļuvi (ja ir auditācijas pieraksti).

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)

5. Nodalīšanas kontrole

Visi Apstrādātāja datu apstrādē piesaistītie pārstāvji Peero lietotnes uzturēšanai izmanto divas datu bāzes: "Kopējie dati" un "Lietotnes dati".

Kopējie dati - Datu bāze, kas ietver informāciju par autorizāciju (t. sk. lietotāju dati - epasti, šifrētas paroles, veiktās autorizācijas lietotnē).

Lietotnes dati - Datu bāze, kas ietver informāciju par lietotnē veiktajām darbībām, iestatījumiem, lietotājiem (t. sk. lietotāju dati - vārds, uzvārds, epasts, valsts, nodaļa, komanda).

6. Integritāte

Auditācijas pieraksti un ziņojumu ģenerēšana sistēmās, lai uzraudzītu darbības sistēmās - kurš ir veicis datu ievadīšanu, izmaiņas vai dzēšanu.

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).

(https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-availability).

The following technical and organisational measures are provided:

- Backup copies
- High accessibility.

Tiek nodrošināti sekojoši tehniskie un organizatoriskie pasākumu:

- Rezerves kopijas
- Augsta pieejamība.

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.

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 Approved Sub-Processors

A list of Approved Sub-Processors is available on site

PEERO DATA SUBPROCESSORS

Latest updates introduced in April 2025

III Apakšapstrādātāji

Apakšapstrādātāju saraksts ir pieejams vietnē

PEERO DATU APAKŠAPSTRĀDĀTĀJI

Pēdējo reizi pārskatīts 2025. gada aprīlī