

Datu aizsardzības procesu vadlīnijas

Šīs vadlīnijas ir izstrādātas, lai nodrošinātu atbilstību Vispārīgajai datu aizsardzības regulai (GDPR) un citām attiecināmām normatīvajām prasībām saistībā ar personīgo datu apstrādi un aizsardzību.

1. Piekļuves kontrole un datu aizsardzība

- **Konta piekļuves ierobežošana:**
 - Katram kontam tiek nodrošināta piekļuve tikai tiem lietotājiem, kam šī piekļuve ir nepieciešama konkrētam mērķim.
 - Piemēram, kontam ar *Erasmus+* datiem ir piekļuve tikai *Erasmus* koordinatoriem, savukārt menedžmenta dati ir pieejami tikai atbildīgajiem vadības darbiniekiem.
- **Regulāra piekļuves pārskatīšana:**
 - Piekļuves tiesības tiek regulāri pārskatītas, lai nodrošinātu, ka tikai pilnvarotas personas var piekļūt konkrētajiem datiem.
 - Nepieciešamības gadījumā piekļuves tiesības tiek pārskatītas un ierobežotas.
- **Tehniskās aizsardzības pasākumi:**
 - Visas sistēmas un konti tiek aizsargāti ar spēcīgām parolēm, divpakāpju autentifikāciju un citām atbilstošām drošības tehnoloģijām.

2. Personas datu apstrādes piekrišana

- **Dalībnieku piekrišana datu apstrādei:**
 - Visi pasākumu dalībnieki, parakstot dalības deklarāciju, apstiprina arī savu personīgo datu apstrādi konkrētam pasākumam un mērķim.
 - Dalības deklarācijā tiek norādīts:
 - Kādi dati tiek apstrādāti (piemēram, vārds, uzvārds, kontaktinformācija).
 - Apstrādes mērķis (piemēram, dalība pasākumā, projektu vadība).
 - Datu glabāšanas termiņš.
- **Caurspīdīgums un informēšana:**
 - Pirms datu apstrādes sākšanas dalībniekiem tiek sniegta skaidra informācija par datu apstrādes mērķiem, apjomu un viņu tiesībām.
 - Dalībniekiem tiek nodrošināta iespēja pieprasīt savu datu dzēšanu vai labošanu, kā arī iesniegt sūdzības.

3. Datu aizsardzības politikas pārvaldība

- **Politikas pārskatīšana un atjaunošana:**
 - Datu aizsardzības vadlīnijas tiek regulāri pārskatītas un pielāgotas, lai nodrošinātu atbilstību jaunākajām normatīvajām prasībām un tehnoloģiskajiem risinājumiem.
- **Apmācības un informētība:**
 - Darbiniekiem, kuriem ir piekļuve personas datiem, tiek nodrošinātas regulāras apmācības par datu aizsardzību un normatīvo aktu prasībām.

- **Incidentu pārvaldība:**

- Ja rodas aizdomas par datu drošības pārkāpumu, tiek veikti nekavējoši pasākumi, lai mazinātu risku un informētu atbildīgās personas vai iestādes.

4. Datu glabāšana un dzēšana

- Personas dati tiek glabāti tikai tik ilgi, cik tas ir nepieciešams konkrētā mērķa sasniegšanai. Pēc tam tie tiek droši dzēsti.
- Glabāšanas termiņi tiek noteikti atbilstoši konkrētā projekta vai pasākuma vajadzībām, ievērojot normatīvos aktus.

Šīs vadlīnijas ir jāievēro visiem darbiniekiem un dalībniekiem, kas iesaistīti datu apstrādē, lai nodrošinātu drošu un atbildīgu personas datu pārvaldību.

Vadlīnijas dalībnieku drošības nodrošināšanai Erasmus+ jauniešu apmaiņas, treniņu un ESC brīvprātīgā darba laikā

Lai nodrošinātu dalībnieku drošību un atbilstību Erasmus+ programmas prasībām, ir svarīgi ievērot šādas vadlīnijas:

1. Dalībnieku drošības plānošana un sagatavošana

1.1. Drošības analīze pirms aktivitātes

- Identificēt iespējamus riskus (piemēram, veselības problēmas, negadījumi, ārkārtas situācijas).
- Izstrādāt drošības plānu, kas ietver preventīvus pasākumus un rīcības soļus ārkārtas gadījumos.

1.2. Atbildīgās personas iecelšana

- Norīkot vienu vai vairākas personas, kas atbild par drošības nodrošināšanu un ārkārtas situāciju vadību.
 - Nodrošināt, lai visiem dalībniekiem ir piekļuve šīm kontaktpersonām.
-

2. Dalībnieku datu ievadīšana sistēmā un dokumentācija

2.1. Laicīga datu ievade

- Visiem dalībniekiem jāiesniedz nepieciešamie personīgie dati (vārds, uzvārds, dzimšanas datums, kontakttālruni, kontaktinformācija ārkārtas gadījumiem).
- Dati jāievada programmas administratīvajās sistēmās ne vēlāk kā divas nedēļas pirms aktivitātes sākuma.

2.2. Konfidencialitātes ievērošana

- Datu apstrādē jāievēro ES Vispārējā datu aizsardzības regula (GDPR).
 - Jānodrošina, ka dati tiek izmantoti tikai drošības un aktivitātes organizēšanas nolūkiem.
-

3. Dalībnieku apdrošināšana

3.1. Apdrošināšanas seguma nodrošināšana

- Visus dalībniekus jāapdrošina ar ceļojuma apdrošināšanu, kas ietver:

Vadlīnijas dalībnieku drošības nodrošināšanai Erasmus+ jauniešu apmaiņas, treniņu un ESC brīvprātīgā darba laikā

Lai nodrošinātu dalībnieku drošību un atbilstību Erasmus+ programmas prasībām, ir svarīgi ievērot šādas vadlīnijas:

1. Dalībnieku drošības plānošana un sagatavošana

1.1. Drošības analīze pirms aktivitātes

- Identificēt iespējamus riskus (piemēram, veselības problēmas, negadījumi, ārkārtas situācijas).
- Izstrādāt drošības plānu, kas ietver preventīvus pasākumus un rīcības soļus ārkārtas gadījumos.

1.2. Atbildīgās personas iecelšana

- Norīkot vienu vai vairākas personas, kas atbild par drošības nodrošināšanu un ārkārtas situāciju vadību.
 - Nodrošināt, lai visiem dalībniekiem ir piekļuve šīm kontaktpersonām.
-

2. Dalībnieku datu ievadīšana sistēmā un dokumentācija

2.1. Laicīga datu ievade

- Visiem dalībniekiem jāiesniedz nepieciešamie personīgie dati (vārds, uzvārds, dzimšanas datums, kontaktāruņi, kontaktinformācija ārkārtas gadījumiem).
- Dati jāievada programmas administratīvajās sistēmās ne vēlāk kā divas nedēļas pirms aktivitātes sākuma.

2.2. Konfidencialitātes ievērošana

- Datu apstrādē jāievēro ES Vispārējā datu aizsardzības regula (GDPR).
 - Jānodrošina, ka dati tiek izmantoti tikai drošības un aktivitātes organizēšanas nolūkiem.
-

3. Dalībnieku apdrošināšana

3.1. Apdrošināšanas seguma nodrošināšana

- Visus dalībniekus jāapdrošina ar ceļojuma apdrošināšanu, kas ietver:



- Medicīniskos izdevumus.
- Negadījumu apdrošināšanu.
- Civiltiesisko atbildību (civiltās atbildības apdrošināšana sedz zaudējumus, kas dalībnieka vainas dēļ nodarīti trešajām personām).

3.2. Apdrošināšanas apliecinājumi

- Organizatoriem jānodrošina, ka visiem dalībniekiem ir spēkā esoši apdrošināšanas polises dokumenti.
 - Dalībniekiem jāizskaidro, kā rīkoties, ja nepieciešama apdrošināšanas izmantošana (piemēram, kur zvanīt ārkārtas gadījumos).
-

4. Drošības pasākumi aktivitāšu laikā

4.1. Informēšana par drošības noteikumiem

- Pirmajā aktivitātes dienā jāveic ievadapmācība par drošības pasākumiem, ieskaitot ugunsdrošību, evakuācijas procedūras un rīcību nelaimes gadījumos.

4.2. Veselības un labklājības uzraudzība

- Jāpārbauda dalībnieku veselības stāvoklis, ja tiek ziņots par diskomfortu vai veselības problēmām.
- Jāsniiedz atbalsts dalībniekiem, ja rodas emocionālās labklājības problēmas (piemēram, izdegšanas simptomi vai kultūras šoks).

4.3. Drošība aktivitāšu laikā

- Nodrošināt, ka aktivitāšu vietas atbilst drošības standartiem.
 - Ja aktivitātes notiek ārpus telpām, jāņem vērā laika apstākļi un citas vides bīstamības.
-

5. Ārkārtas situāciju pārvaldība

5.1. Rīcības plāns ārkārtas situācijām

- Izstrādāt procedūras negadījumu, dabas katastrofu, vai cita veida ārkārtas gadījumiem.
- Iepriekš izplānot sakaru kanālus ar vietējām iestādēm (piemēram, policiju, medicīnas palīdzību).

5.2. Ziņošana un sekojošā analīze

- Pēc jebkura incidenta jāiesniedz ziņojums par notikušo, analizējot situāciju un ieteicot uzlabojumus nākotnei.

Šīs vadlīnijas palīdzēs nodrošināt gan organizatoru, gan dalībnieku drošību, kā arī sekmēs sekmīgu un efektīvu programmas īstenošanu.