

Apstiprināts

BSA Senāta

2019. gada. 23. oktobrī
protokols Nr.140

Baltijas Starptautiskās akadēmijas Privātuma politika

Izdoti saskaņā ar Vispārīgo datu aizsardzības regulu un
Fizisko personu datu apstrādes likumu

1. Vispārīgie noteikumi

- 1.1. Šī BSA privātuma politika (turpmāk – Politika) reglamentē SIA “Baltijas Starptautiskā akadēmija” , reģistrācijas numurs: 40003101808, juridiskā adrese: Lomonosova iela 4, Rīga, LV-1003, kontaktinformācija par personas datu aizsardzības jautājumiem: Lomonosova iela 4, Rīga, LV-1003, it@bsa.edu.lv (turpmāk – datu pārzinis) galvenos principus un noteikumus par personas datu vākšanu, apstrādi un glabāšanu un datu pārziņa tīmekļa vietnes www.bsa.edu.lv (turpmāk – tīmekļa vietne) ekspluatācijas noteikumiem.
- 1.2. Datu subjekts šajā Politikā ir jebkura fiziska persona, kuras personas dati tiks reģistrēti tīmekļa vietnē.
- 1.3. Datu pārzinis ievēro šos datu apstrādes principus:
 - 1.3.1. Personas datus apstrādā likumīgi, taisnīgi un pārredzami attiecībā uz datu subjektu;
 - 1.3.2. Personas datus vāc precīzi, skaidrā un leģitīmā nolūkā, nevis tālāk apstrādā veidā, kas nav saderīgs ar šiem mērķiem; turpmāka apstrāde arhivēšanas nolūkos sabiedrības interesēs, zinātniskos vai vēsturiskos pētījumos vai statistikas nolūkos netiek uzskatīta par nesaderīgu ar sākotnējiem mērķiem;
 - 1.3.3. Personas dati ir adekvāti, atbilstīgi un ietver tikai to, kas nepieciešams to apstrādes nolūkos;
 - 1.3.4. Personas dati ir precīzi un, ja nepieciešams, tiek atjaunināti; jāveic visi pamatotie pasākumi, lai nodrošinātu to, ka personas dati, kas ir neprecīzi, ņemot vērā mērķus, kuriem tie tiek apstrādāti, tiek nekavējoties dzēsti vai laboti;
 - 1.3.5. Personas datus glabā tādā formā, kas ļauj identificēt datu subjektus ne ilgāk kā tas ir nepieciešams; personas datus var uzglabāt ilgāk, ciktāl personas datus apstrādās tikai arhivēšanas nolūkos sabiedrības interesēs, zinātniskos vai vēsturiskos pētījumos vai statistikas nolūkos, uz kuriem attiecas atbilstīgu tehnisko un organizatorisko pasākumu īstenošana, kas vajadzīgi, lai aizsargātu tiesības un brīvības datu subjektu;
 - 1.3.6. Personas datus apstrādā tā, lai nodrošinātu pienācīgu personas datu drošību, tostarp aizsardzību pret neatļautu vai nelikumīgu apstrādi un

nejaušu pazaudēšanu, iznīcināšanu vai bojājumu, izmantojot atbilstošus tehniskus vai organizatoriskus pasākumus;

- 1.3.7. Datu pārzinis ir atbildīgs par iepriekš minētajiem principiem un spēj pierādīt to atbilstību.
- 1.3.8. Izmantojot trešo pušu pakalpojumus, var tikt piemēroti trešo pušu noteikumi un nosacījumi. Tāpēc, izmantojot šo trešās puses pakalpojumus, ieteicams iepazīties ar piemērojamajiem noteikumiem un nosacījumiem.
- 1.3.9. Šī Politika ir sagatavota saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46 / EK (Vispārīgā datu aizsardzības regula, turpmāk tekstā – GDPR), un piemērojamie Latvijas Republikas normatīvie akti.

2. Personas datu vākšana, apstrāde un uzglabāšana

- 2.1. Datu subjekts piekrīt un neiebilst savu personas datu pārvaldīšanai un apstrādei, ko veic datu pārzinis, saskaņā ar privātuma Politikas un tiesību aktos noteiktajām procedūrām.
- 2.2. Ievadot savus personas datus, datu subjekts piešķir datu pārzinim tiesības apkopot, sistematizēt, lietot un pārvaldīt savus personas datus, kas nodoti tieši vai netieši apmeklējot mājas lapu, jebkādam mērķim, kas minēts šajā privātuma Politikā.
- 2.3. Datu subjekts ir atbildīgs par to, lai sniegtie dati būtu precīzi, pareizi un pilnīgi. Apzināti nepareizu datu ievadīšana tiek uzskatīta par privātuma Politikas pārkāpumu. Ja iesniegtie dati mainās, datu subjektam tie nekavējoties jālabo un, ja šādas iespējas nav, jāinformē par to datu pārzini. Datu pārzinis un apstrādātājs nav atbildīgs par datu subjektam un / vai trešajām personām radītajiem zaudējumiem, ja datu subjekts ir iesniedzis nepareizus un / vai nepilnīgus personas datus vai nav pieprasījis datu pievienošanu un / vai grozīšanu pēc viņu maiņas.

3. Personas datu apstrāde

- 3.1. Datu pārzinis - nodibinājums IT izglītības fonds nodrošina diva veida saturu:
 - 3.1.1. Datorikas saturu akadēmijas personālam un studentiem;
 - 3.1.2. Moodle kursus, zināšanu pārbaudes testus par apgūtajiem kursiem un apgūto zināšanu apliecinājuma visiem interesentiem.
- 3.2. Reģistrējoties "BSA e-studiju vide" sadaļā kā *students* Jums būs jānorāda informācija par sevi: Vārds, Uzvārds, E-pasts.
- 3.3. Reģistrējoties "BSA e-studiju vide" sadaļā kā *akadēmiskais personāls*, Jums būs jānorāda informācija par sevi: Vārds, Uzvārds, E-pasts.
- 3.4. Pieslēdzoties ar "BSA e-studiju vide" uz tevi attiecas privātuma politika.
- 3.5. Personas datu apstrādes juridiskais pamats ir GDPR 6. panta 1. punkta a) apakšpunkts (apstrāde ar Kandidāta piekrišanu), b) apakšpunkts (apstrāde līguma izpildei vai lai veiktu darbību pēc Kandidāta iniciatīvas pirms līguma noslēgšanas).

4. Personas datu uzglabāšanas procedūras un termiņi, datu krātuves un pārsūtīšanas vietas

- 4.1. Datu apstrādātājs, apstrādājot un uzglabājot datu subjektu personas datus, īsteno organizatoriskus un tehniskus pasākumus, kas nodrošinātu personas datu aizsardzību no nejaušanas vai nelikumīgas iznīcināšanas, pārveidošanas, izpaušanas un jebkādiem citiem nelikumīgas apstrādes līdzekļiem.
- 4.2. Datu apstrādātājs apkopo jūsu personas datus tik ilgi, cik ilgi jūs izmantojat mūsu pakalpojumus, kā arī saskaņā ar spēkā esošajiem noteikumiem. Datu apstrādātājs nekādā veidā neapņemas glabāt visus jūsu datus nenoteikta laika perioda garumā. Jūs varat piekļūt dažiem datiem (Vārds, Uzvārds, E-pasts, Tālruna numurs, Dzimšanas datums), kamēr jums ir aktīvs konts pie mums. Dati var tikt izdzēsti jebkurā brīdī jūsu aktīvās konta izmantošanas laikā saskaņā ar iepriekš tekstā izklāstītajiem noteikumiem.
- 4.3. Datu apstrādātājam piederoši serveri un trešo pušu serveri (datu centrs), kuros datu apstrādātājs apstrādā un uzglabā datus, atrodas tikai Eiropas Savienības teritorijā (Latvija). Datu apstrādātājs apņemas nepārsūtīt nekādus datus ārpus Eiropas Ekonomikas zonas.

5. Datu subjekta tiesības

- 5.1. Datu subjektiem ir GDPR garantētās datu subjekta tiesības un ar šo Politiku šīs tiesības netiek ierobežotas vai samazinātas. Datu subjektiem jebkurā brīdī, iesniedzot pieprasījumu, ir tiesības iepazīties ar personas datiem, ko apstrādā datu pārzinis, un saņemt informāciju par to apstrādi, īstentot savas tiesības labot savus neaktuālos, nepilnīgos, nepareizos personas datus, lūgt apturēt personas datu apstrādes darbības, ja datu apstrāde neatbilst likumiem un šīs Politikas prasībām.
- 5.2. Ciktāl personas datu apstrāde notiek, pamatojoties uz piekrišanu, Datu subjektam ir tiesības jebkurā laikā atsaukt piekrišanu, neietekmējot tādas apstrādes likumīgumu, kuras pamatā ir pirms atsaukuma sniegta piekrišana.
- 5.3. Datu subjekti var izmantot savas esošās tiesības, iesniedzot rakstisku pieteikumu pa e-pastu: it@bsa.edu.lv vai pa pastu uz adresi Rīga, Lomonosova iela 4, Rīga, LV-1003 vai tieši apmeklējot datu pārziņa biroju darba laikā. Datu pārzinis var prasīt papildus identificējošu vai pamatojošu informāciju, ja tā konkrētā gadījumā uzskatāma par nepieciešamu un samērīgu.
- 5.4. Ja datu subjekts nav apmierināts ar datu pārziņa darbībām un uzskata, ka datu pārzinis apstrādājis datu subjekta personas datus tādā veidā, kas neatbilst juridiskajām prasībām, datu subjekts var iesniegt sūdzību Datu valsts inspekcijā.

6. Informācija par sīkdatņu (cookies) izmantošanu

- 6.1. Datu pārziņa interneta vietne izmanto sīkdatnes. Sīkdatne ir maza apjoma teksta faili, kas tiek glabāti vietnes apmeklētāja pārlūkprogrammā vai ierīcē (personālais dators, mobilais tālrunis vai planšetdators).
- 6.2. Pateicoties sīkdatnēm, mēs cenšamies nodrošināt patīkamāku pieredzi cilvēkiem, kuri pārlūko vietni un uzlabo vietni.
- 6.3. Tīmekļa vietnē izmantotās sīkdatnes var grupēt šādos veidos:

- 6.3.1. Funkcionālās sīkdatnes (startit_session, start_it_courses_session) ir izstrādātas, lai ļautu interneta vietnei izpildīt savas galvenās funkcijas. Šīs sīkdatnes ļauj pārlūkot vietni un izmantot vēlamās funkcijas.
- 6.3.2. Darbības (analītiskās) sīkdatnes (_utma, _utmz, _utmc, _utmb, _utmt / Google Analytics) apkopo anonīmu informāciju par to, kā apmeklētāji izmanto interneta vietni. Sniedzot informāciju par apmeklētajām vietnēm, par tīmekļa vietnē pavadīto laiku un iespējamām problēmām, piemēram, par kļūdas ziņojumiem, šīs sīkdatnes palīdz datu pārzinim saprast, kā apmeklētāji uzvedas tīmeklī. Šī informācija palīdz uzlabot tīmekļa vietnes darbību.
- 6.4. Datu subjekts var izdzēst vai bloķēt sīkdatnes, atlasot attiecīgos iestatījumus pārlūkprogrammā, kas ļauj bloķēt visas vai dažas sīkdatnes. Ir zināms, ka, izmantojot pārlūkprogrammas iestatījumus, kas bloķē visas sīkdatnes (ieskaitot nepieciešamās), var tikt radītas problēmas, izmantojot visas vai daļu no vietnes funkcijām. Papildu informāciju par sīkdatnēm, kā arī kā tās iespējams pārvaldīt vai izdzēst, varat iegūt mājaslapā www.aboutcookies.org.

7. Risku pārvaldība

- 7.1. Drošības politikā ietvertās risku pārvaldības normas ir izstrādātas, lai mazinātu apdraudējumu līmeni un tiktu nodrošināta informācijas konfidencialitāte, integritāte un pieejamība, kā arī, lai mazinātu iespējamus zaudējumus.
- 7.2. Balstoties uz informācijas resursu klasifikāciju, tiek veikta risku pārvaldība. Plānojot risku pārvaldīšanas pasākumus, IT sistēmu drošības pārvaldnieks, sadarbojoties ar resursu turētājiem, veic IS risku analīzi.
- 7.3. Risku analīzes mērķis ir novērtēt:
- 7.3.1. IS apdraudējuma īstenošanās varbūtību, kur IS apdraudējums ir ar nodomu vai aiz neuzmanības izdarīta darbība vai bezdarbība, vai iespējams notikums, kas var izraisīt informācijas dzēšanu, noklusēšanu, informācijas resursu vai tehnisko resursu maiņu, bojāšanu vai informācijas nonākšanu personu rīcībā, kas nav tam pilnvarotas;
- 7.3.2. iespējamo kaitējumu informācijas resursu turētājam vai BSA, ja nav nodrošināta pietiekama IS drošība.
- 7.4. Risku analīzi regulāri (ne retāk kā reizi gadā) veic visām IS, kā arī katram jaunam ar IS saistītam projektam un IS, kurām veiktas izmaiņas, kas var ietekmēt IS drošību. Analizējot riskus, jāņem vērā aktuālākā situācija attiecībā uz IS aizsardzības pasākumiem.
- 7.5. Saskaņā ar risku analīzes rezultātiem tiek sagatavots risku pārvaldības plāns par drošības pasākumu ieviešanu kā arī pilnveidots sistēmu darbības nepārtrauktības un atjaunošanas plāns.
- 7.6. Risku analīzi veic, lietojot risku analīzes metodiku, kas ir noteikta BSA informācijas sistēmu drošības risku vadības noteikumos

8. Nobeiguma noteikumi

- 8.3. Ar šo Politiku saistītās tiesiskās attiecības reglamentē GDPR un piemērojamie Latvijas Republikas normatīvie akti.
- 8.4. Datu pārzinis nav atbildīgs par zaudējumu atlīdzību, ieskaitot zaudējumus, kas radušies tīmekļa vietnes lietošanas traucējumu, datu bojājumu vai datu zuduma dēļ,

kas izriet no Datu subjekta darbības vai bezdarbības, vai trešajām personām, kas rīkojas Datu subjekta vārdā, ieskaitot nepareizu ievadi dati, citas kļūdas, apzināta ļaunprātīga rīcība un cita nelikumīga tīmekļa vietnes izmantošana. Datu pārzinis arī neuzņemas atbildību par jebkādu mājas lapas ieiešanas / izmantošanas un (vai) bojājumu rezultātā radušos traucējumus, kas rodas no trešo personu darbības vai bezdarbības, kas nav saistīti ar datu subjektu, ieskaitot problēmas ar elektroenerģiju, piekļuvi internetam , utt.

- 8.5. Datu pārzinim ir tiesības jebkurā laikā daļēji vai pilnīgi mainīt šo Politiku.
- 8.6. Politikas izmaiņas vai papildinājumi stājas spēkā dienā, kad tās publicētas datu pārziņa Tīmekļa vietnē.
- 8.7. Ja Datu subjekts turpina izmantot Tīmekļa vietni un datu pārziņa pakalpojumus pēc tam, kad Politika ir atjaunināta vai mainīta, tiek pieņemts, ka Datu subjekts piekrīt šādiem papildinājumiem un / vai izmaiņām.

Dokumenta datums un versija: spēkā no 26.10.2019.