VIDZEMES AUGSTSKOLA

Cēsu iela 4,
Valmiera, LV-4200
T.: +371 64207230,
F: +371 64207229
info@va.lv, www.va.lv

LV90001342592
Valsts Kase
LV38TREL9150130000000
TRELLV22

Vidzemes Augstskolas
personas datu apstrādes aizsardzības noteikumi

1. Noteikumu mērķis

1.1. Personas datu apstrādes aizsardzības noteikumi (turpmāk – Noteikumi) izstrādāti saskaņā ar 2016.gada 27.aprīļa Eiropas Parlamenta un Eiropas Savienības Padomes Personas datu aizsardzības regulu Nr.2016/679 (turpmāk – Regula) un citiem normatīvajiem aktiem, kas reglamentē fizisko personu datu aizsardzību un personas datu apstrādi.

1.2. Noteikumi izstrādāti ar mērķi noteikt personas datu aizsardzības prasības Vidzemes Augstskolā (turpmāk – ViA), darbiniekiem un visām tām personām, kas ViA uzdevumā uz noslēgto līgumu pamata vai pilnvarojuma veic personas datu apstrādi, lai tiktu ievērotas un izpildītas Regulas un citu LR normatīvo aktu prasības, lai personas datu apstrāde notiktu tam paredzētajam mērķim un nepieciešamajā apjomā, nodrošinot godprātīgu personas datu apstrādi, kā arī lai noteiktu visus pamatotos pasākumus personas datu aizsardzībā.

2. Noteikumos lietoto terminu skaidrojums

2.1. **Pārzinis** – ViA, kuru pārstāv rektors, kurš nosaka personas datu apstrādes mērķus, uzdevumus, apstrādes līdzekļus, kā arī atbild par personas datu apstrādi saskaņā ar Regulu un šiem Noteikumiem.

2.2. **Datu subjekts** - fiziskā persona, kuru var tieši vai netieši identificēt un kura sniedz ViA savus personas datus.

2.3. **Personas dati** - jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu (datu subjektu), kuru var tieši vai netieši identificēt (piemēram, personas vārds, uzvārds, identifikācijas numurs, atrašanās vietas dati, fiziskai personai raksturīgie fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktori).

2.4. **Personas datu apstrāde** - jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem (piemēram, datu vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana, pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus; saskaņošana, kombinēšana, ierobežošana, dzēšana vai iznīcināšana).

2.5. **Personas datu saņēmējs** - fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kurai izpauž personas datus.

2.6. **Trešā persona** - fiziska vai juridiska persona, publiska iestāde, aģentūra vai struktūra, kura nav datu subjekts, pārzinis, apstrādātājs un personas, kuras pārziņa vai apstrādātāja tiešā pakļautībā ir pilnvarotas apstrādāt personas datus.

2.7. **Personas datu lietotājs** - darbinieks, kurš atrodas darba tiesiskajās attiecībās ar Pārzini vai ar kuru Pārzinim ir citas līgumattiecības, un kurš ir Pārziņa norīkots veikt personas datu apstrādi, izmantojot noteiktas Personu datu apstrādes sistēmas, kā arī kurš ir rakstiski apliecinājis ievērot normatīvo aktu prasības attiecībā uz fizisko personu datu aizsardzību un šos Noteikumus, un kurš ir saņēmis Pārziņa atļauju veikt personas datu apstrādi.

2.8. **Personas datu apstrādes sistēma** - strukturizēts informācijas tehnoloģiju un datu bāzu kopums, fiksēts elektroniski, papīra, manuālā vai jebkādā citā formā; kas veidots ar mērķi sistematizēti uzkrāt personas datus, izmantojot personas datu apstrādi.

2.9. **Personas datu sistēmas drošība** - informācijas pieejamības, integritātes (pilnīgas un neizmainītas informācijas saglabāšana) un konfidencialitātes (informāciju saņem tikai tam pilnvarotas personas) nodrošināšana Personas datu apstrādes sistēmā.

2.10. **Personas datu sistēmas apdraudējums** - ar nodomu, tīši vai aiz neuzmanības izdarīta darbība vai bezdarbība, vai nepārvaramas varas apstākļu (ugunsgrēks, plūdi, neatbilstoša temperatūra, elektroenerģijas padeves traucējumi, personas datu zādzība vai nelikumīga personas datu iegūšana vai izmantošana) rezultātā iestājies notikums, kas var izraisīt personas datu dzēšanu, izmainīšanu, pazušanu, noklusēšanu, informācijas resursu vai

tehnisko resursu izmaiņas, bojāšanu vai personas datu nonākšanu trešo personu rīcībā, kuras nav tam pilnvarotas vai kurām nav paredzēts saņemt personas datus.

2.11. **Fiziskā aizsardzība** - tehnisko resursu aizsardzība pret fiziskas iedarbības radītu Personas datu sistēmas apdraudējumu.

2.12. **Loģiskā aizsardzība** – aizsardzība, kuru realizē ar programmatūras līdzekļiem, identificējot Pārzini vai personas datu lietotāju, pārbaudot viņa pilnvaru atbilstību attiecīgajām darbībām Personas datu sistēmā, pasargājot personas datus no tīšas vai nejaušas izmainīšanas vai dzēšanas.

2.13. **Parole** – Pārzinim un/vai personas datu lietotājam zināma simbolu virkne, kuras kopija atrodas sistēmā un, kuru izmantojot, var atvērt noteiktas programmas, datoru, personas datu apstrādes sistēmas.

3. Pamatnoteikumi personas datu apstrādē

3.1. Personas datu lietotājiem jāievēro šādi principi:

3.1.1. personas datu apstrādei jābūt godprātīgai un likumīgai;

3.1.2. personas datu apstrāde jāveic tikai atbilstoši paredzētajam mērķim un tam nepieciešamajā apjomā;

3.1.3. personas datu glabāšanas laikam un veidam ir jābūt tādam, kas datu subjektu ļauj identificēt attiecīgā laika posmā, kurš nepārsniedz paredzētajam datu apstrādes mērķim noteikto laika posmu, kā arī ievērojot ViA Lietu nomenklatūrā paredzētos dokumentu glabāšanas termiņus;

3.1.4. personas datu apstrādē jāievēro datu pareizība un to savlaicīga atjaunošana, labošana vai dzēšana, ja personas dati ir nepilnīgi vai neprecīzi.

3.2. Personas datu apstrādi, piekļūšanu tehniskajiem resursiem, kas tiek izmantoti personu datu apstrādei un aizsardzībai, kā arī personas datu apstrādē izmantotos resursus pārvieto tikai tam pilnvarotas personas, t.sk. personas datu lietotāji.

3.3. Nododot personas datus, tiek saglabāta informācija par:

3.3.1. personas datu nodošanas laiku (piemēram, nosūtīšanas laiks ir redzams e-pastā);

3.3.2. personu, kura nodevusi personas datus (piemēram, e-pastā tiek uzglabāta informācija par nosūtītāju);

3.3.3. personu, kura saņēmusi personas datus (piemēram, e-pastā tiek uzglabāta informācija par saņēmēju).

3.4. Saņemot personas datus, tiek saglabāta informācija par:

3.4.1. personas datu saņemšanas laiku (piemēram, saņemšanas laiks ir redzams e-pastā, kā arī laiks tiek reģistrēts interneta datubāzē);

3.4.2. personu, kura nodevusi personas datus (piemēram, e-pastā tiek uzglabāta informācija par nosūtītāju);

3.4.3. personu, kura saņēmusi personas datus (piemēram, e-pastā tiek uzglabāta informācija par saņēmēju).

3.5. ViA apņemas ievērot šādus datu apstrādes labas prakses principus:

3.5.1. dati tiek godīgi un likumīgi apstrādāti;

3.5.2. datu apstrāde tiek veikta konkrētiem mērķiem un tikai saskaņā ar tiem;

3.5.3. dati ir adekvāti (ne pārmērīgi) un dati ir precīzi;

3.5.4. dati netiek glabāti ilgāk kā nepieciešams.

3.5.5. dati tiek apstrādāti saskaņā ar datu subjekta tiesībām;

3.5.6. dati ir drošībā;

3.5.7. dati netiek pārsūtīti citām juridiskām personām vai uz ārvalstīm bez drošas adekvātas aizsardzības.

4. Personas datu subjekti, personas datu veidi

4.1. ViA ir šādi Personas datu subjekti:

4.1.1. darbinieki;

4.1.2. studenti;

4.1.3. sadarbības partneri.

4.2. Personas datu apstrādē tiek apstrādāti šādi personas datu veidi:

4.2.1. darbinieku personas dati;

4.2.2. grāmatvedības dati;

4.2.3. studentu personas dati;

4.2.4. sadarbības partneru dati;
4.2.5. videonovērošanā fiksētie personas dati.

5. Personas datu sistēmas, to klasifikācija

5.1. Personas datu aizsardzības klasifikācija tiek veidota atkarībā no personas datu vērtības un konfidencialitātes pakāpes, kuras tiek klasificētas atkarībā no kaitējuma, kāds varētu tikt nodarīts konkrētam datu subjektam un tā personas datiem.

5.2. ViA ir šādas Personas datu sistēmas ar noteiktām to riska un konfidencialitātes pakāpēm:

Nr.	*Personas datu sistēmas veids*	*Riska pakāpe*	*Konfidencialitātes pakāpe*	*Atbildīgā persona ViA par Personas datu sistēmu*
1.	Darbinieku personas datu apstrādes sistēma	Vidēja riska	Augsta konfidencialitāte	Pārzinis (ViA rektors vai rektora deleģēta persona)
2.	Grāmatvedības datu apstrādes sistēma	Vidēja riska	Augsta konfidencialitāte	Pārzinis (ViA rektors vai rektora deleģēta persona)
3.	Studentu personas datu apstrādes sistēma	Vidēja riska	Augsta konfidencialitāte	Pārzinis (ViA rektors vai rektora deleģēta persona)
4.	Videonovērošanas datu apstrādes sistēma	Vidēja riska	Augsta konfidencialitāte	Pārzinis (ViA rektors vai rektora deleģēta persona)

5.3. Pārzinis var pārskatīt katras Personas datu apstrādes sistēmas vērtības, ja mainās Pārziņa organizatoriskā, tehnoloģiskā, ekonomiskā vai cita darbība, kā arī gadījumos, kad tiek mainīts apstrādājamo Personas datu saturs vai vērtība.

6. Personas datu apstrādes informācijas un tehniskie resursi

6.1. Personas datu apstrādi un tehnisko aizsardzību īsteno ar fiziskiem un loģiskiem aizsardzības līdzekļiem, nodrošinot aizsardzību pret fiziskās iedarbības radītu personas datu apdraudējumu, kā arī aizsardzību, kuru realizē ar programmatūras līdzekļiem, parolēm u.c. loģiskās aizsardzības līdzekļiem.

6.2. Personas datu apstrāde tiek nodrošināta ar šādiem tehniskiem resursiem: dators, datortīkla aparatūra, sistēmprogrammas, lietojumprogrammas, sistēmfaili, datu faili u.c. biroja tehnika.

6.3. Personas datu lietotājiem katram ir savs stacionārais vai portatīvais dators. Personas datu apstrādei tiek izmantoti arī citi tehniskie resursi (piemēram, kopētājs, faksa aparāts, skeneris u.c. biroja tehnika).

7. Atbildīgās personas par resursiem, personas datu lietotāji, to tiesības, pienākumi, ierobežojumi un atbildība

7.1. Atbildīgā persona par personas datu aizsardzību ViA kopumā ir Pārzinis (kuru pārstāv ViA rektors).

7.2. Atbildīgā persona par informācijas resursiem (t.i., atbildība par resursu sadali, nepieciešamo informācijas resursu nodrošināšanu, resursu funkcionalitātes izvērtēšanu, utt.) ir Pārzinis (kuru pārstāv ViA rektors) un atbildīgo struktūrvienību/struktūrgrupu vadītāji.

7.3. Atbildīgā persona par tehniskajiem resursiem (t.i., atbildība par informācijas tehnoloģijām, par tehnikas esamību un funkcionēšanu, utt.) ir Pārzinis (kuru pārstāv ViA rektors) un IT grupas vadītājs.

7.4. Atbildīgā persona par personas datu aizsardzību - personas datu lietotājs. Šo statusu darbinieks iegūst pēc darba līguma noslēgšanas, iepazīstoties ar amata aprakstu, šiem Noteikumiem, parakstot iesniegumu par darba tiesisko attiecību uzsākšanu un uzņemoties atbildību par personas datu aizsardzību un šo Noteikumu ievērošanu.

7.5. Personas datu lietotājam nav atļauts Personas datu sistēmā esošos personas datus izpaust (pilnībā vai daļēji) trešajām personām, nodot tos, atsavināt, kopēt, pārvietot, pārveidot, dzēst un veikt jebkādas citas darbības, sniegt jebkādas rakstiskas, mutiskas vai telefoniskas ziņas par personas datiem no Personas datu sistēmām.

7.6. Personas datu Lietotājs nedrīkst nodot trešajām personām lietotāja rekvizītus (lietotāja vārdu un paroli). Lietotāja rekvizītus drīkst izmantot tikai konkrētais lietotājs (fiziska persona), kuram tie piešķirti.
7.7. Ziņas no Personas datu sistēmas drīkst sniegt tikai šajos Noteikumos paredzētajā kārtībā, lai ievērotu personas datu apstrādes mērķi.
7.8. Personas datu lietotājam ir tiesības ar Pārziņa norādījumu un/vai saskaņojumu izpaust un nodot personas datus valsts/pašvaldību pārvaldes iestādēm, kurām normatīvajos aktos ir piešķirtas tiesības pieprasīt un saņemt šādu informāciju, kā arī tad, kad normatīvie akti prasa noteiktā laikā, termiņā un kārtībā sniegt attiecīgus personas datus, statistiskās atskaites vai citas ziņas, pie nosacījuma, ja tas ietilpst personas datu lietotāja amata pienākumos.
7.9. Personas datu lietotājs atbild par šajos Noteikumos noteikto ierobežojumu un personas datu konfidencialitātes saistību ievērošanu arī pēc darba tiesisko attiecību izbeigšanas.
7.10. Neievērojot šajos Noteikumos noteiktās personas datu aizsardzības prasības, kā arī Regulu un citus normatīvos aktus attiecībā par fizisko personu datu aizsardzību, Personas datu lietotājam var iestāties disciplinārā, civiltiesiskā vai krimināla atbildība un pienākums segt nodarītos tiešos zaudējumus.
7.11. Jebkādu informāciju/datus, kas kļūst pieejami personas datu lietotājiem, veicot savus darba pienākumus, ja šāda informācija ir saistīta ar Pārzini un tā darbību, studentiem vai sadarbības partneriem, uzskata par Pārzinim piederošu un konfidenciālu informāciju, ko aizsargā atbilstoši piemērojamie normatīvie akti par konfidenciālas informācijas, komercnoslēpumu un personas datu aizsardzību.
7.12. Nododot personas datus uz valstīm, kas nav Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstis, jāizvērtē, vai attiecīgā valsts nodrošina pietiekamu personas datu aizsardzības līmeni. Ja attiecīgā valsts nenodrošina pietiekamu personas datu aizsardzības līmeni, ir jāsaņem attiecīgā datu subjekta piekrišana personas datu nosūtīšanai. Ja attiecīgā valsts nodrošina pietiekamu personas datu aizsardzības līmeni, datu subjekts rakstveidā jāinformē par datu nosūtīšanu.
7.13. Personas datu lietotāji personas datu aizsardzības Noteikumus vai grozījumus tajos saņem elektroniski uz ViA elektronisko pastu no Lietvedības informācijas sistēmas un apņemas tos ievērot (ViA Darba kārtības noteikumi, 18.8.punkts: Informācija, kas saņemta elektroniski no Lietvedības informācijas sistēmas, uzskatāma par nodotu no darba devēja puses un pieņemts, ka darbinieks ar to ir iepazinies).

8. Drošības pasākumi, pārtraucot uz laiku darbu vai beidzot darbu

8.1. Personas datu lietotājam pārtraucot darbu uz laiku un atstājot darba telpas, pārbaudīt, vai nepiederošām trešajām personām viegli pieejamā veidā nav atstāti dokumenti, kas satur personu datus. Dokumentus novietot skapī un aizslēgt tā durvis, ja skapis ir slēdzams.
8.2. Personas datu lietotājam pārtraucot darbu, datoru atstāt tādā stāvoklī, lai darbu varētu atsākt tikai pēc informācijas sistēmas lietotāja autentificēšanas.
8.3. Beidzot darbu darba dienas beigās:
- 8.3.1. noglabāt (datora komanda „*Save*") visus atvērtos dokumentus un/vai programmas, kurās tiek apstrādāti personas dati;
- 8.3.2. aizvērt visas datorprogrammas;
- 8.3.3. datoru izslēgt vai atstāt tādā stāvoklī, lai darbu varētu atsākt tikai pēc informācijas sistēmas lietotāja autentificēšanas;
- 8.3.4. sakārtot savu darbavietu – dokumentus, kas satur personas datus, novietot skapī un ieslēgt tos, ja tas ir iespējams, nokārtot galda virsmu, atbrīvojot to no liekiem dokumentiem;
- 8.3.5. nevajadzīgos dokumentus vēlreiz pārbaudīt, un, ja tie nav vairāk vajadzīgi, tad iznīcināt dokumentu smalcinātājā;
- 8.3.6. aizvērt visus telpas logus un aizslēgt sava kabineta durvis.

9. Personas datu dzēšana

9.1. Datu subjektam ir tiesības panākt, lai pārzinis bez nepamatotas kavēšanās dzēstu datu subjekta personas datus, un pārziņa pienākums ir bez nepamatotas kavēšanās dzēst personas datus, ja pastāv viens no šādiem nosacījumiem:

9.1.1. personas dati vairs nav nepieciešami saistībā ar nolūkiem, kādos tie tika vākti vai citādi apstrādāti;
9.1.2. datu subjekts atsauc savu piekrišanu, uz kuras pamata veikta apstrāde;
9.1.3. datu subjekts iebilst pret apstrādi un apstrādei nav nekāda svarīgāka leģitīma pamata;
9.1.4. personas dati ir apstrādāti nelikumīgi;
9.1.5. personas dati ir jādzēš, lai nodrošinātu, ka tiek pildīts juridisks pienākums, kas noteikts Eiropas Savienības vai dalībvalsts tiesību aktos.

9.2. Ja pārzinis ir publiskojis personas datus un tā pienākums saskaņā ar Noteikumiem ir minētos personas datus dzēst, pārzinis, ņemot vērā pieejamo tehnoloģiju un tās piemērošanas izmaksas, veic saprātīgus pasākumus, tostarp tehniskus pasākumus, lai informētu pārziņus, kas veic personas datu apstrādi, ka datu subjekts ir pieprasījis, lai minētie pārziņi dzēstu visas saites uz minētajiem personas datiem vai minēto personas datu kopijas vai atveidojumus.

9.3. Dati netiek dzēsti, ciktāl apstrāde ir nepieciešama:
9.3.1. lai īstenotu tiesības uz vārda brīvību un informāciju;
9.3.2. lai izpildītu juridisku pienākumu, kas prasa veikt apstrādi, kā paredzēts Savienības vai dalībvalsts tiesību aktos, kuri piemērojami pārzinim, vai lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai saistībā ar pārzinim likumīgi piešķirto oficiālo pilnvaru īstenošanu;
9.3.3. pamatojoties uz sabiedrības interesēm sabiedrības veselības jomā;
9.3.4. arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, vai statistikas nolūkos saskaņā ar 89. panta 1. punktu, ciktāl 1. punktā minētās tiesības varētu neļaut vai būtiski traucēt sasniegt minētās apstrādes mērķus;
9.3.5. lai celtu, īstenotu vai aizstāvētu likumīgas prasības.

10. Rīcība bīstamās un ārkārtas situācijās

10.1. Ja ir notikusi jebkāda veida iejaukšanās Personas datu apstrādes sistēmā, personas datu zādzība, nelikumīga nodošana trešajām personām, kurām tie nav paredzēti, datu bojāšana vai jebkādas citas pretlikumīgas darbības ar personu datiem, jebkāds ārkārtas gadījums (ugunsgrēks, plūdi, elektrības pārrāvums, u.c.), Personas datu lietotājam jāievēro šādi noteikumi:
10.1.1. nekavējoties informēt par notikušo Pārzini, izstāstot notikuma būtību, apstākļus, kā arī nodarīto kaitējumu;
10.1.2. veikt visas savu iespēju un saprāta robežās iespējamās darbības, lai atgūtu nozaudētos, pazaudētos vai prettiesiski izpaustos personas datus;
10.1.3. veikt visas normatīvajos aktos paredzētās darbības, lai novērstu, mazinātu kaitējuma sekas, t.i., zvanīt policijai, ugunsdzēsējiem u.c. atbildīgajām institūcijām;
10.1.4. aktīvi iesaistīties personas datu glābšanas, saglabāšanas pasākumos – sniegt visu zināmo informāciju par notikušo un par jebko, kas varētu palīdzēt novērst kaitējumu;
10.1.5. pārtraukt darbu ar tiem darba priekšmetiem, kas var apdraudēt pašu Personas datu lietotāju, personas datus un citas personas;
10.1.6. saglabāt darba vietu tādā stāvoklī, kādā tā bija notikuma brīdī, ja tā rezultātā netiek vēl vairāk bojāti personas dati;
10.1.7. savu iespēju robežās, neapdraudot savu un citu darbinieku drošību, veselību un dzīvību, veikt visus iespējamos pasākumus, lai apdraudētos datus glābtu no briesmām (izņemt no ūdens, nogādāt drošā, sausā vietā, pārnest uz citu telpu, u.tml.).

11. Citi noteikumi

11.1. Pārzinim ir pienākums kontrolēt, lai datiem var piekļūt tikai tie darbinieki, kam tas ir nepieciešams darba pienākumu veikšanai.
11.2. Pēc darbinieka darba tiesisko attiecību pārtraukšanas elektroniskie faili, kas satur personas datus, jādzēš pēc vai šie dati jāanonimizē.
11.3. Sensitīvo personas datu apstrāde jānodala no pārējo personas datu apstrādes.
11.4. Jāsaņem darbinieku rakstveida atļauja izglītības dokumentu, fotogrāfiju un CV glabāšanai, vai šie dati jāiznīcina.