IZRAKSTS

Datu valsts inspekcija

Blaumaņa iela 11/13-15, Rīga, LV-1011, tālr. 67223131, fakss 67223556, e-pasts info@dvi.gov.lv, www.dvi.gov.lv

Rīgā

Rīgas Stradiņa universitātei
(nosūtīšanai e-adreses informācijas sistēmā)

Informācijai:
Rīgas Stradiņa universitātes
datu aizsardzības speciālistei
[…]
[…]@rsu.lv

Lēmums

Rīgā, 2020.gada 1.jūlijā Nr.2-2.2/17

Par pienākuma uzlikšanu un rājiena izteikšanu

Datu valsts inspekcija 2020.gada 7.maijā nosūtīja Rīgas Stradiņa universitātei (turpmāk – RSU) 2020.gada 7.maija vēstuli Nr.3-4.5/107-N, kurā lūdza sniegt šajā vēstulē minēto informāciju un norādīja, ka tās rīcībā ir informācija, kā arī par to liecina publiski pieejama informācija (https://nra.lv/latvija/izglitiba-karjera/312498-pandemijas-laika-izaicinajumiem-augstskolas-pielagojusas.htm un https://www.rsu.lv/studejosajiem-respondus-monitor-un-lockdown-parluka-lietosana), ka RSU pandēmijas laikā, nodrošinot apmācību procesu, t.sk. pārbaudījumu kārtošanu attālināti, izmanto LockDown Browser pārlūku un Respondus Monitor platformu.

Publiski pieejamā informācija liecina, ka LockDown Browser pārlūks integrēts ar E-studijām, kas nodrošina piemērotu vidi attālinātai pārbaudījumu vai testu kārtošanai. Tas nozīmē, ka papildus programmas vai interneta pārlūkus atvērt nav iespējams, kamēr tiek kārtots pārbaudījums. Šī programma tiek izmantota tikai pārbaudījumu veikšanai E-studijās. Savukārt Respondus Monitor platforma nodrošina pakalpojumu, kas pārbauda studentu identitāti pirms pārbaudījuma, pēc tam veic videoierakstu caur Web kameru, kamēr studenti kārto pārbaudījumu. Programmatūra izmanto mākslīgā intelekta algoritmus, lai atzīmētu aizdomīgus mirkļus par studentu uzvedību pārbaudījuma laikā, kurus lektoriem ir jāpārskata videoierakstā. Šī programma ļauj automātiski noteikt studentu uzvedību, kas varētu liecināt par krāpšanos pārbaudījumu laikā. Programmatūra var norādīt, ka students ir izgājis no istabas, otrās personas ienākšanu vai citas uzvedības problēmas.

Datu valsts inspekcija 2020.gada 18.maijā saņēma RSU 2020.gada 18.maija vēstuli Nr.60-6/217/2020 *(Datu valsts inspekcijā saņemta un reģistrēta 2020.gada 18.maijā ar Nr.3-4.5/152-S)* (turpmāk – Vēstule), kurā ietvertas atbildes uz Datu valsts inspekcijas 2020.gada 7.maija vēstulē Nr.3-4.5/107-N uzdotajiem jautājumiem.

Izvērtējot RSU Vēstulē sniegto informāciju, Datu valsts inspekcijai radās papildu jautājumi attiecībā uz RSU veikto personas datu apstrādi, izmantojot Respondus Monitor

platformu un šīs apstrādes atbilstību Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 par fizisko 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 – Regula) prasībām.

Ievērojot minēto, Datu valsts inspekcija 2020.gada 28.maijā plkst.10:00 veica pārbaudi klātienē RSU telpās. Pārbaudes mērķis bija pārliecināties par RSU izmantotajām Respondus Monitor rīka funkcionalitātēm, noskaidrot lēmuma pieņemšanas procesu un pamatotību attiecībā uz attiecīgā rīka izmantošanu pārbaudījumu veikšanas procesā. Tāpat Datu valsts inspekcija klātienē precizēja atsevišķus RSU Vēstulē sniegtās informācijas aspektus, tai skaitā attiecībā uz personas datu apstrādes tiesisko pamatu.

[1] RSU savā Vēstulē norāda, ka RSU ieskatā ne Respondus Monitor, ne RSU neveic biometrisko datu apstrādi.

Pārbaudē klātienē tika konstatēts, ka Respondus Monitor platformas izmantošanas laikā tiek pieprasīts apstiprināt, ka studējošā web kamera strādā, tad jāapstiprina testa video, tad seko instrukcija, kas jādara, izmantojot platformu (piemēram, izslēgt radio, televizoru, nevajag gulēt dīvānā u.c.), tiek pieprasīts uzrādīt studenta apliecību, tad Respondus Monitor platformas programma pārbauda personu (salīdzina studenta attēlu videoierakstā ar studenta apliecībā esošo bildi). Ja persona ir ārpus kameras vai kustās, tad sistēma paziņo, ka identitāte neatbilst. Tāpat tika konstatēts, ka, veicot pārbaudījuma videoierakstu, Respondus Monitor platformā uz videoieraksta laika celiņa ar sarkanu krāsu tiek atzīmētas studenta aizdomīga darbība (piemēram, students ir izgājis no telpas, telpā iegāja vēl viena persona utt.).

Tāpat tika konstatēts, ka arī Respondus, Inc savā tīmekļa vietnē https://web.respondus.com/he/monitor/ *(uzklikšķinot uz "**Monitor AI** is the most advanced artificial intelligence system for automated proctoring")* norāda, ka Respondus Monitor platformas centrā ir jaudīgs mākslīgā intelekta dzinējs Monitor AI™, kas katru sekundi veic eksāmena sesijas analīzi. Pirmais Monitor AI slānis ietver uzlabotus algoritmus sejas detektoram, kustībai un apgaismojumam, lai analizētu studentu un eksāmenu vidi. Nākamajā slānī tiek izmantoti dati no skaitļošanas ierīces (tastatūras darbība, peles kustības, aparatūras izmaiņas utt.), lai identificētu ar krāpšanos saistītus modeļus un anomālijas. Visbeidzot, studenta mijiedarbība ar pašu eksaminācijas instrumentu ir iestrādāta analīzē, ieskaitot katra jautājuma salīdzināšanu ar citiem studentiem, kas veikuši to pašu eksāmenu.

Kopumā Monitor AI analizē desmitiem faktoru, piemēram, video kadrā ir redzamas viena vai vairākas sejas un, ja persona, kas sākusi eksāmenu, samainās vietām ar citu personu. Pēc tam dati nonāk "Review Priority" sistēmā, lai instruktoriem palīdzētu ātri novērtēt rezultātus.

Datu valsts inspekcija informē, ka darba grupa personu aizsardzībai attiecībā uz personas datu apstrādi (kas izveidota, pamatojoties uz Eiropas Parlamenta un Padomes 1995.gada 24.oktobra Direktīvas 95/46/EK "Par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti" 29.pantu) (turpmāk – Darba grupa) savā atzinumā 3/2012 "Par biometrijas tehnoloģiju attīstību" norāda, ka ir divas galvenās biometrijas metožu kategorijas:

- pirmkārt, ir fiziski un fizioloģiski pamatotas metodes, ar kurām mēra personas fiziskās un fizioloģiskās īpašības un pie kurām pieder pirkstu nospiedumu pārbaude, pirkstu attēlu analīze, varavīksnenes atpazīšana, tīklenes analīze, sejas atpazīšana, plaukstas ģeometrija, ausu formas atpazīšana, ķermeņa aromāta konstatēšana, balss atpazīšana, DNS paraugu analīze, sviedru poru analīze utt.;

- otrkārt, ir ar uzvedību pamatotas metodes, ar kurām mēra personas uzvedību un pie kurām pieder ar roku rakstīta paraksta pārbaude, taustiņsitienu analīze, gaitas, iešanas vai kustēšanās veida analīze, uzvedības modeļi, kas norāda uz zemapziņas domāšanu, piemēram, melošanu, utt.

Būtu jāņem vērā arī jaunā psiholoģiski pamatotu metožu joma. Tā ietver atbildes reakcijas mērījumus konkrētās situācijās un specifiskus testus attiecībā uz atbilstību psiholoģiskam profilam".

Papildus iepriekš minētajam Datu valsts inspekcija vērš uzmanību, ka Eiropas datu aizsardzības kolēģijas 2020.gada 29.janvāra viedoklī 3/2019 "Par personas datu apstrādi,

izmantojot videoierīces" norādīts, ka biometrisko datu izmantošana un jo īpaši sejas atpazīšana rada paaugstinātu risku datu subjekta tiesībām. Ir būtiski, lai šādu tehnoloģiju izmantošana notiktu, pienācīgi ievērojot tiesiskuma, nepieciešamības, samērīguma un datu minimizācijas principus, kas izklāstīti Regulā. Pārzinim vispirms būtu jāizvērtē ietekme uz pamattiesībām un brīvībām un jāapsver mazāk traucējoši līdzekļi, lai sasniegtu apstrādes likumīgo mērķi.

Lai personas datus kvalificētu kā "biometriskos datus" Regulas izpratnē, jēldatu apstrādei, ir jāietver mērījumus par fiziskas personas fiziskās, fizioloģiskās vai uzvedības īpašībām. Tā kā biometriskie dati ir šādu mērījumu rezultāts, Regulas 4.panta 14) apakšpunktā noteikts, ka "[…], pēc specifiskas tehniskas apstrādes, kuri attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm, kas ļauj veikt vai apstiprina minētās fiziskās personas unikālu identifikāciju […]". Tomēr personas video ierakstu nevar uzskatīt par biometriskiem datiem saskaņā ar 9.pantu, ja tas nav īpaši tehniski apstrādāts, lai palīdzētu identificēt personu.

Lai biometrisko datu apstrādi varētu uzskatīt par īpašu kategoriju personas datu apstrādi (Regulas 9.pants), ir nepieciešams, lai biometriskie dati tiktu apstrādāti "ar mērķi unikāli identificēt fizisku personu".

Rezumējot, ņemot vērā Regulas 4.panta 14) apakšpunktu un 9. pantu, jāņem vērā trīs kritēriji:

- datu veids: dati, kas attiecas uz fiziskas personas fiziskām, fizioloģiskām vai uzvedības īpašībām,
- apstrādes līdzekļi un veids: dati, kas "iegūti īpašas tehniskas apstrādes rezultātā",
- apstrādes mērķis: dati jāizmanto, lai unikāli identificētu fizisku personu.

Regulas 51.apsvērumā norādīts, ka fotogrāfiju *(pēc analoģijas arī video ierakstu)* apstrāde nebūtu sistemātiski jāuzskata par īpašu kategoriju personas datu apstrādi, jo uz tām biometrisko datu definīcija attiecas tikai tad, kad tās apstrādās ar konkrētiem tehniskiem līdzekļiem, kas ļauj veikt fiziskas personas unikālu identifikāciju vai autentifikāciju. Šādi personas dati nebūtu jāapstrādā, ja vien apstrāde nav atļauta konkrētos, šajā regulā precizētos gadījumos, ņemot vērā, ka dalībvalstu tiesību aktos var būt paredzēti konkrēti noteikumi par datu aizsardzību, lai pieņemtu šīs regulas noteikumu piemērošanu juridisku pienākumu izpildei vai sabiedrības interesēs veiktu uzdevumu izpildei, vai pārzinim likumīgi piešķirto oficiālo pilnvaru īstenošanai. Papildus konkrētajām prasībām attiecībā uz šādu apstrādi būtu jāpiemēro vispārējie principi un citi šīs regulas noteikumi, jo īpaši attiecībā uz likumīgas apstrādes nosacījumiem. Būtu skaidri jāparedz atkāpes no vispārējā aizlieguma apstrādāt šādu īpašu kategoriju personas datus, cita starpā tad, ja datu subjekts dot nepārprotamu piekrišanu, vai attiecībā uz īpašām vajadzībām, jo īpaši gadījumos, kad apstrādi veic konkrētas apvienības vai nodibinājumi savu leģitīmo darbību ietvaros, kuru nolūks ir atļaut īstenot pamatbrīvības.

Ņemot vērā iepriekš minēto, Datu valsts inspekcija konstatē, ka Respondus Monitor platforma īpaši tehniski apstrādā personas datus, lai unikāli identificētu studentu *(salīdzina attēlu video ierakstā ar studenta apliecībā esošo attēlu)* un konstatētu aizdomīgas darbības. Līdz ar to Datu valsts inspekcija secina, ka tiek veikta biometrisko datu *(personas dati pēc specifiskas tehniskas apstrādes, kuri attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm, kas ļauj veikt vai apstiprina minētās fiziskās personas unikālu identifikāciju, piemēram, sejas attēli vai daktiloskopijas dati)* apstrāde, kas tiek uzskatīta par īpašu kategoriju datu apstrādi.

[2] Pārbaudē klātienē, kā arī savas Vēstules 8.punktā RSU norādīja, ka tiesiskais pamats atbilstoši RSU veiktajai personas datu apstrādei, izmantojot Respondus Monitor platformu, ir Regulas 6.panta 1.punkta a) apakšpunkts – datu subjekts ir devis piekrišanu savu personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem. Ja persona (studējošais) nav piekritis personas datu apstrādei, Respondus Monitor izmantošana nav iespējama un tiek meklēts cits, alternatīvs pārbaudījumu kārtošanas veids.

RSU iesniegtajā 2020.gada 8.aprīļa rektora rīkojuma Nr.5-1/152/2020 "Par komisijas izveidi attālināto gala pārbaudījumu norises nodrošināšanai" 1.punktā norādīts, ka: "*Lai*

turpinātu RSU studiju procesu Latvijas Republikā izsludinātās ārkārtējās situācijas apstākļos un nolūkā nodrošināt attālināto gala pārbaudījumu norises kārtību un saturu, noteikts veikt platformas Respondus Monitor izmantošanu rakstveida gala pārbaudījumu nodrošināšanai un platformas Zoom izmantošanu mutisko gala pārbaudījumu nodrošināšanai."

Datu valsts inspekcija nekonstatē, ka minētais rīkojuma punkts pieļauj studentiem izvēlēties, kādā veidā un izmantojot kādus resursus kārtot eksāmenu. Minētais rīkojuma punkts konkrēti nosaka RSU kārtību attiecībā uz eksāmenu kārtošanu.

Arī RSU tīmekļa vietnē (https://www.rsu.lv/studejosajiem-respondus-monitor-un-lockdown-parluka-lietosana) publiski pieejamā informācija neliecina, ka students var piekrist vai nepiekrist personas datu apstrādei, izmantojot Respondus Monitor platformu.

Pārbaudē klātienē, RSU paskaidroja, ka studentiem pastāv arī alternatīvie rīki eksāmenu kārtošanai, piemēram, kārtot eksāmenu klātienē, izmantot ZOOM programmu vai kārtot eksāmenu attālināti, izmantojot visus materiālus, bet tad eksāmens būs sarežģītāks. Tāpat pārbaudē klātienē RSU paskaidroja, ka studentam ir tiesības pirms kārtot eksāmenu, izmantot Respondus Monitor platformu testa režīmā, kura laikā, students var iepazīties ar platformas funkcionalitāti, un lietošanas noteikumiem, lai izvērtētu savas iespējas kārtot eksāmenu, izmantojot šo platformu. Arī RSU tīmekļa vietnes (https://www.rsu.lv/studejosajiem-respondus-monitor-un-lockdown-parluka-lietosana) punktā "Izmēģiniet LockDown Browser mēģinājuma testu" ir skaidrots, ka *Studējošajiem ir iespēja laikus sagatavoties pārbaudījumam un kārtot izmēģinājuma testu. Aicinām to darīt savlaicīgi (vismaz nedēļu iepriekš) un pārliecinieties, ka dators sakonfigurēts korekti. Testu var kārtot neierobežotu reižu skaitu. Ja gadījumā ir kāda problēma, lūdzu vērsties pēc tehniskās konsultācijas IT Servisa centrā vai informēt studiju kursa docētāju.* Tāpat skaidrojošā informācija ir pieejama arī sadaļā BUJ Studējošajiem pie jautājuma "Kā studējošie izmantos Respondus Monitor, lai kārtotu pārbaudījumu". Tāpat RSU norādīja, ka pasniedzējs informē par iespējamiem eksāmena kārtošanas rīkiem, kā arī pats students individuāli var vienoties ar pasniedzēju par citiem eksāmena kārtošanas rīkiem.

Līdz ar to Datu valsts inspekcija neguva pierādījumus tam, ka studenti var brīvi izvēlēties, izmantojot kādus rīkus, viņi vēlētos kārtot eksāmenus. Tādejādi ir konstatējams, ka attiecībā uz eksāmena kārtošanas rīku izvēli, RSU nenodrošina pietiekamu studentu informēšanu par iespēju atteikties no konkrētas platformas lietošanas un lietot citus rīkus.

Ievērojot minēto, Datu valsts inspekcija paskaidro, ka Regulas 6.panta 1.punkts nosaka, ka apstrāde ir likumīga tikai tādā apmērā un tikai tad, ja ir piemērojams vismaz viens no turpmāk minētajiem pamatojumiem: a) datu subjekts ir devis piekrišanu savu personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem; b) apstrāde ir vajadzīga līguma, kura līgumslēdzēja puse ir datu subjekts, izpildei vai pasākumu veikšanai pēc datu subjekta pieprasījuma pirms līguma noslēgšanas; c) apstrāde ir vajadzīga, lai izpildītu uz pārzini attiecināmu juridisku pienākumu; d) apstrāde ir vajadzīga, lai aizsargātu datu subjekta vai citas fiziskas personas vitālas intereses; e) apstrāde ir vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras; f) apstrāde ir vajadzīga pārziņa vai trešās personas leģitīmo interešu ievērošanai, izņemot, ja datu subjekta intereses vai pamattiesības un pamatbrīvības, kurām nepieciešama personas datu aizsardzība, ir svarīgākas par šādām interesēm, jo īpaši, ja datu subjekts ir bērns.

Savukārt pirms biometrisko datu apstrādes uzsākšanas, ir svarīgi ņemt vērā Regulas 9.panta 1.punktu, kas nosaka, ka ir aizliegta biometrisko datu apstrāde. Tomēr, Regulas 9.panta 2.punktā ir iekļauti izņēmumi biometrisko datu apstrādē, un tā ir pieļaujama, piemēram, ja datu subjekts ir devis nepārprotamu piekrišanu šo personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem, izņemot, ja Savienības vai dalībvalsts tiesību akti paredz, ka 1.punktā minēto aizliegumu datu subjekts nevar atcelt.

Saskaņā ar Regulas 4.panta 11) apakšpunktu datu subjekta "piekrišana" ir jebkura brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu personas datu apstrādei. Līdz ar to piekrišana ir jādod ar skaidri apstiprinošu darbību, kas nozīmē brīvi sniegtu,

konkrētu, apzinātu un viennozīmīgu norādi par datu subjekta piekrišanu ar viņu saistīto personas datu apstrādei, piemēram, ar rakstisku, tostarp elektronisku, vai mutisku paziņojumu.

Regulas 7.panta 1.punkts paredz, ka, ja apstrāde pamatojas uz piekrišanu, pārzinim ir jāspēj uzskatāmi parādīt, ka datu subjekts ir piekritis savu personas datu apstrādei. Savukārt minēta panta 3.punkts nosaka, ka datu subjektam ir tiesības atsaukt savu piekrišanu jebkurā laikā. Piekrišanas atsaukums neietekmē apstrādes likumību, kas pamatojas uz piekrišanu pirms atsaukuma. Datu subjektam jābūt par to informētam, pirms viņš dod savu piekrišanu. Atsaukt piekrišanu ir tikpat viegli kā to dot.

Tāpat Datu valsts inspekcija norāda uz Regulas 32.apsvērumu, kurš noteic, ka piekrišana būtu jādod ar skaidri apstiprinošu darbību, kas nozīmē brīvi sniegtu, konkrētu, apzinātu un viennozīmīgu norādi par datu subjekta piekrišanu ar viņu saistīto personas datu apstrādei, piemēram, ar rakstisku, tostarp elektronisku, vai mutisku paziņojumu. Tas varētu ietvert laukuma atzīmēšanu ar ķeksīti interneta tīmekļa vietnē, informācijas sabiedrības pakalpojumu tehnisko iestatījumu izvēli vai citu paziņojumu vai rīcību, kas šajā gadījumā skaidri norāda, ka datu subjekts piekrīt piedāvātajai savu personas datu apstrādei. Klusēšana, iepriekš atzīmēti laukumi vai atturēšanās no darbības tādējādi nebūtu jāuzskata par piekrišanu. Piekrišanai būtu jāattiecas uz visām apstrādes darbībām, ko veic vienā un tajā pašā nolūkā vai nolūkos. Ja apstrādei ir vairāki nolūki, piekrišana būtu jādod visiem nolūkiem. Ja datu subjekta piekrišana ir jādod pēc elektroniska pieprasījuma, pieprasījumam jābūt skaidram, kodolīgam, un tam nav nevajadzīgi jāpārtrauc tā pakalpojuma izmantošana, par ko tas tiek sniegts.

Vienlaikus Datu valsts inspekcija informē, ka Darba grupas izstrādātajās Vadlīnijās par jēdziena "piekrišana" definīciju (Guidelines on Consent under Regulation 2016/679 (wp259rev.01), kas ir pieejamas tīmekļa vietnē http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (turpmāk – Vadlīnijas) ir detalizēti skaidroti piekrišanas nosacījumi un to būtība. Vadlīnijās norādīts, ka piekrišana var būt pienācīgs tiesiskais pamats, ja datu subjektam tiek piedāvāta viņa piekrišanas izmantošanas kontrole un patiesas izvēles iespēja pieņemt vai noraidīt piedāvājumu, dot savu piekrišanu bez kaitīgām sekām datu subjektam, kurš noraidījis piekrišanas došanu. Piedāvājot datu subjektam dot piekrišanu, pārzinim ir jānovērtē, vai piekrišana atbildīs visām prasībām derīgas piekrišanas iegūšanai (Regulas 7.pants un 8.pants). Ja piekrišana ir iegūta pilnībā atbilstoši Regulas prasībām, tas ir instruments, kurš piešķir datu subjektam tiesības veikt kontroli, vai viņa personas dati tiks vai netiks apstrādāti. Ja šādas kontroles iespējas datu subjektam netiek piedāvātas, kontrole kļūst iluzora un piekrišana ir uzskatāma par nederīgu tiesisko pamatu personas datu apstrādei. Darba grupa norāda, ka piekrišanai ir jābūt labprātīgi (brīvi) sniegtai, kas nozīmē savās spējās neierobežota indivīda brīvprātīga lēmuma pieņemšanu, kuru neietekmē nekādi spaidi (piespiešana). Vienlaikus uzsverot, ka piekrišana var būt spēkā gadījumos, kad datu subjektam ir reālas izvēles iespējas bez maldināšanas, iebiedēšanas, piespiešanas vai ievērojamu negatīvu seku radīšanas, ja persona nepiekrīt datu apstrādei. Ja piekrišanas sekas mazina indivīda izvēles brīvību, tad piekrišana nav sniegta labprātīgi. Turklāt ikvienu piekrišanu ikviens var atsaukt, izņemot, ja datu apstrāde ir saistīta ar līgumsaistību izpildi. Datu valsts inspekcija vērš uzmanību, ka būtisks priekšnoteikums piekrišanas atbilstībai ir iepriekšēja datu subjekta informēšana par personas datu apstrādi ievērojot Regulas 13.pantā noteikto obligāti sniedzamo informācijas kopumu.

Ņemot vērā iepriekš minēto, Datu valsts inspekcija konstatē, ka RSU, iegūstot piekrišanu no studentiem, nav pilnvērtīgi ievērojusi Regulas prasības piekrišanas saņemšanai. Proti, ir konstatējams, ka RSU iegūstot piekrišanu, nepietiekami informē studentus par viņu personas datu apstrādi.

[3] Datu valsts inspekcija, izvērtējot RSU sniegto informāciju Datu valsts inspekcijai adresētajās vēstulēs, pārbaudē klātienē, kā arī ievērojot publiski un Datu valsts inspekcijas rīcībā pieejamo informāciju, konstatē, ka RSU nav pietiekami nodrošinājusi datu subjektu (studentu) informēšanu atbilstoši Regulas prasībām, proti, RSU tīmekļa vietnē https://www.rsu.lv/studejosajiem-respondus-monitor-un-lockdown-parluka-lietosana nav pieejama Regulas 13.pantā minēta informācija. Minētajā tīmekļa vietnē ir pieejama atsauce uz

Respondus, Inc izstrādāto privātuma politiku, kura ir pieejama tikai angļu valodā. Līdz ar to konstatējams arī, ka RSU un Respondus, Inc sniegtā informācija nav viegli pieejama studentiem. Informācijas izvietošanas struktūra neatbilst Regulas prasībām *(Regulas 58.apsvērums – pārredzamības principa pamatā ir prasība, ka visa informācija, kas adresēta sabiedrībai vai datu subjektam, ir kodolīga, viegli pieejama un viegli saprotama un ka tiek izmantota skaidra un vienkārša valoda un papildus – vajadzības gadījumā – vizualizācija. […])*. Konkrētajā gadījumā, lai iegūtu informāciju par savu personas datu apstrādes mērķi, datu glabāšanas termiņu u.c. ir jāveic vairākas darbības.

Regulas 5.pants nosaka personu datu apstrādes principus, kas pārzinim jāievēro, veicot personu datu apstrādi. Regulas 5.panta 1.punkta a) apakšpunktā noteikts, ka personas dati tiek apstrādāti likumīgi, godprātīgi un datu subjektam pārredzamā veidā ("likumīgums, godprātība, un pārredzamība"). Pārredzamības principa tiesiskais regulējums noteikts Regulas III nodaļā (Datu subjekta tiesības). Regulas 12.pantā ir izklāstīti vispārīgie principi, kas attiecas uz: informācijas sniegšanu datu subjektiem (saskaņā ar 13.–14.pantu); saziņu ar datu subjektiem saistībā ar viņu tiesību īstenošanu (saskaņā ar 15.–22.pantu); un saziņu saistībā ar datu aizsardzības pārkāpumiem (34.pants). Pārredzamības princips sevī ietver datu subjekta tiesības būt informētam un Regulas 12.pants nosaka, ka *pārzinis veic atbilstošus pasākumus, lai kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu, datu subjektam sniegtu visu 13. un 14. pantā minēto informāciju [..]*, no kā izriet, ka pārzinim ir pienākums nodrošināt datu subjektu ar iespēju pārraudzīt datu apstrādi. Regulas 58.apsvērums nosaka, ka pārredzamības principa pamatā ir prasība, ka visa informācija, kas adresēta sabiedrībai vai datu subjektam, ir kodolīga, viegli pieejama un viegli saprotama un ka tiek izmantota skaidra un vienkārša valoda un papildus – vajadzības gadījumā – vizualizācija. Šādu informāciju var sniegt elektroniski, piemēram, darot to pieejamu sabiedrībai tīmekļa vietnē. Tas ir jo īpaši svarīgi situācijās, kad iesaistīto personu skaits un praksē izmantoto tehnoloģiju sarežģītība apgrūtina datu subjekta iespējas zināt un saprast, vai tiek vākti viņa personas dati, kas to dara un kādā nolūkā. Ņemot vērā, ka bērniem pienākas īpaša aizsardzība, ja apstrāde attiecas uz bērnu, informācija būtu jāsniedz un saziņa jāveic tik skaidrā un vienkāršā valodā, lai bērns to varētu viegli saprast.

Darba grupa Pārredzamības pamatnostādnēs saskaņā ar Regulu (turpmāk – Pamatnostādnes) skaidro pārredzamības principa īstenošanu.

Attiecīgi Regulas 12.panta 1.punkts nosaka, ka pārredzama informācija ir tāda, kas ir kodolīga, pārredzama un viegli pieejama. Pamatnostādnes nosaka, ka *"Vieglas pieejamības" elements nozīmē, ka datu subjektam nevajadzētu būt spiestam meklēt informāciju; viņiem uzreiz ir jābūt redzamam, kur un kā var piekļūt šai informācijai, piemēram, tieši to sniedzot viņiem, nodrošinot saiti uz to, skaidri norādot to vai kā atbildei uz dabiskās valodas jautājumu, piemēram, tiešsaistes vairāku līmeņu paziņojums par datu aizsardzību, sadaļā "Biežāk uzdotie jautājumi,"* no kā izriet, ka viens no efektīvākajiem pārredzamības principa īstenošanas paņēmieniem ir informācijas (kas nodrošina datu subjektu ar informāciju par viņa datu apstrādi) publicēšana iestādes tīmekļa vietnē.

Ņemot vērā iepriekš minēto, ***Datu valsts inspekcija konstatē, ka RSU veiktajā personas datu apstrādē, izmantojot Respondus Monitor platformu, ir nepietiekama personas datu apstrādes pārredzamības principa nodrošināšana un informācijas trūkums***.

[4] RSU savā Vēstulē norāda, ka *RSU ieskatā ne Respondus Monitor, ne RSU neveic personas profilēšanu vai biometrisko datu apstrādi atbilstoši šajā un turpmākajos punktos sniegtajam skaidrojumam, tādēļ pirms personas datu apstrādes uzsākšanas, izmantojot Respondus Monitor platformu, novērtējums par ietekmi uz datu aizsardzību nav veikts. […] Ciktāl RSU ir izdevies uzzināt no Respondus informācijas resursiem, Respondus Monitor šie identifikācijas dati netiek nodoti un Respondus Monitor ierakstus un to uzglabāšanu veic kodētā veidā, piešķirot savu sesijas identifikācijas kodu.*

Tāpat Datu valsts inspekcijas rīcībā esošā informācija liecina, ka RSU pirms personas datu apstrādes, izmantojot Respondus Monitor platformu, nav izvērtējusi samērīgumu pret

personu privātumu.

4.1. Datu valsts inspekcija paskaidro, ka, ievērojot Regulas 5.panta 2.punktā noteikto pārskatatbildības principu, tieši pārzinim (RSU) ir pienākums nodrošināt tādu personas datu apstrādes procesu, kas ļauj pierādīt, ka pārziņa veiktā personas datu apstrāde ir atbilstoša datu aizsardzības normatīvā regulējuma prasībām.

Paskaidrojam, ka pirms personas datu apstrādes uzsākšanas ir jāizvērtē tās mērķis un samērīgums pret personu privātumu. Informējam, ka veiktajai datu apstrādei ir jābūt līdzsvarotai un balansētai. Balansēšanu jāveic, ņemot vērā datu subjekta (studentu) un pārziņa (RSU) interešu līdzsvarošanu. Balansēšanu datu apstrādes veicējam jāizstrādā, ņemot vērā datu subjekta un pārziņa interešu līdzsvarošanu. Interešu līdzsvarošana veicama, sākotnēji definējot nolūku, kura sasniegšanai datu apstrāde nepieciešama (nolūkam jābūt likumīgam, skaidram un reālam), jāveic novērtējums, kādēļ mērķa sasniegšanai nepieciešama personas datu apstrāde (piemēram, kādēļ mērķi nav iespējams sasniegt, izmantojot personas privātumu mazāk skarošus līdzekļus), jāveic sākotnējais līdzsvara novērtējums (apstrādātāja interešu veids (komercintereses, sabiedrības intereses, pamattiesības u.c.)), jānovērtē potenciālais kaitējums, ja apstrāde netiek veikta, datu subjekta statuss (piemēram, nepilngadīgais, pensionārs, nodarbinātais), datu apstrādes veids, datu subjekta tiesību aizskāruma lielums, datu subjekta pamatotās gaidas, ietekmes samērojums ar labumu), piemērotie papildu drošības pasākumi (datu minimizācija, ieviestie tehniskie un organizatoriskie pasākumi u.c.), pārredzamības nodrošināšana, citu datu subjekta tiesību nodrošināšana. Ja minētais process nav veikts, personas datu apstrāde neatbildīs Regulas prasībām. Vēršam uzmanību arī uz to, ka studentiem, t.sk. kārtojot pārbaudījumus, ir tiesības uz privātās dzīves neaizskaramību. RSU ir jārespektē studentu privātā dzīve. Tādējādi ir nepieciešams nodrošināt proporcionalitāti starp studentu tiesībām un RSU interesēm.

Papildus norādāms, ka atbilstoši Regulas 24.panta 1. un 2.punktam, ņemot vērā apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisku personu tiesībām un brīvībām, pārzinim jāīsteno atbilstoši tehniskie un organizatoriskie pasākumi, lai nodrošinātu un spētu uzskatāmi pierādīt, ka apstrāde notiek saskaņā ar Regulu. Tādējādi saprotams, ka RSU jānodrošina tehniskos un organizatoriskos līdzekļus, lai datu apstrāde būtu droša.

Regulas 83.apsvērumā norādīts, ka, lai saglabātu drošību un novērstu tādu apstrādi, kurā tiek pārkāpta šī regula, pārzinim vai apstrādātājam būtu jānovērtē apstrādei raksturīgie riski un jāīsteno pasākumi šo risku mazināšanai, piemēram, šifrēšana. Minētajiem pasākumiem, ņemot vērā tehniskās iespējas un īstenošanas izmaksas, būtu jānodrošina atbilstošs drošības līmenis, tostarp konfidencialitāte, attiecībā uz apstrādei raksturīgo risku un aizsargājamo personas datu īpatnībām. Novērtējot datu drošības risku, vērā būtu jāņem riski, ko rada personas datu apstrāde, piemēram, nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem, kas var izraisīt fizisku, materiālu vai nemateriālu kaitējumu.

Regulas 84.apsvērumā minēts, ka, lai sekmētu šīs regulas noteikumu ievērošanu gadījumos, kad apstrādes darbības varētu izraisīt augstu risku fizisku personu tiesībām un brīvībām, pārzinim vajadzētu būt atbildīgam par novērtējuma par ietekmi uz datu aizsardzību veikšanu, lai jo īpaši izvērtētu minētā riska avotus, raksturu, specifiku un nopietnību. Novērtējuma rezultāti būtu jāņem vērā, nosakot piemērotus pasākumus, kas veicami, lai uzskatāmi parādītu, ka personas datu apstrāde atbilst šai regulai.

Ņemot vērā iepriekš minēto, norādām, ka RSU ir jāveic RSU veiktās personas datu apstrādes atbilstības izvērtējums Regulas prasībām, t.sk. vērtēt iespējamos riskus fizisku personu tiesībām un brīvībām.

Regulas 75.apsvērumā tiek skaidrots, ka risku fizisku personu tiesībām un brīvībām – ar atšķirīgu iespējamību un nopietnību – var radīt personas datu apstrāde, kas var izraisīt fizisku, materiālu vai nemateriālu kaitējumu, jo īpaši, ja apstrāde var izraisīt diskrimināciju, identitātes zādzību vai viltošanu, finansiālu zaudējumu, kaitējumu reputācijai, ar dienesta noslēpumu aizsargātu personas datu konfidencialitātes zaudēšanu, neatļautu pseidonimizācijas atcelšanu vai

jebkādu citu īpaši nelabvēlīgu ekonomisko vai sociālo situāciju; ja datu subjektiem var tikt atņemtas viņu tiesības un brīvības vai atņemta iespēja kontrolēt savus personas datus; ja tiek apstrādāti personas dati, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību, piederību arodbiedrībai, un ja tiek apstrādāti ģenētiskie dati, veselības dati vai dati par dzimumdzīvi, vai sodāmību un pārkāpumiem vai ar tiem saistītiem drošības pasākumiem; ja tiek izvērtēti personiskie aspekti, jo īpaši analizējot vai prognozējot aspektus attiecībā uz personas sniegumu darbā, ekonomisko situāciju, veselību, personīgām vēlmēm vai interesēm, uzticamību vai uzvedību, atrašanās vietu vai pārvietošanos, lai izveidotu vai izmantotu personiskos profilus; ja tiek apstrādāti neaizsargātu fizisku personu, īpaši bērnu, personas dati; vai ja apstrāde ietver lielu personas datu daudzumu un ietekmē lielu skaitu datu subjektu.

Informējam, ka Regulas 35.panta 1.punkts nosaka, ka, ja apstrādes veids, jo īpaši, izmantojot jaunās tehnoloģijas un ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūkus, varētu radīt augstu risku fizisku personu tiesībām un brīvībām, pārzinis pirms apstrādes veic novērtējumu par to, kā plānotās apstrādes darbības ietekmēs personas datu aizsardzību. Darba grupa savās izstrādātajās pamatnostādnēs "Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA) veikšanai un noskaidrošanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē" norāda, ka novērtējums par ietekmi uz datu aizsardzību ir process, kas izveidots tā, lai aprakstītu apstrādi, novērtētu tās nepieciešamību un samērīgumu un palīdzētu pārvaldīt tādus riskus fizisku personu tiesībām un brīvībām, kas izriet no personas datu apstrādes, novērtējot tos un nosakot pasākumus to novēršanai. Novērtējumi par ietekmi uz datu aizsardzību ir svarīgi pārskatatbildības rīki, jo tie palīdz pārziņiem ne vien nodrošināt atbilstību Regulas prasībām, bet arī parādīt, ka ir veikti atbilstošie pasākumi, lai panāktu atbilstību Regulai (sk. arī 24.pantu). Proti, novērtējums par ietekmi uz datu aizsardzību ir atbilstības nodrošināšanas un pierādīšanas process.

Datu valsts inspekcija vērš uzmanību, ka galvenais apstāklis, kas jāņem vērā pārzinim, analizējot, vai ir veicams novērtējums par ietekmi uz datu aizsardzību, ir augsts risks fiziskas personas tiesībām un brīvībām. Papildus iepriekš minētajam Regulas 35.panta 3.punktā ir norādīti trīs gadījumi, kad pārzinim jo īpaši būtu jāvērtē augsta riska personu tiesībām un brīvībām iestāšanās, proti: a) ar fiziskām personām saistītu personisku aspektu sistemātiska un plaša novērtēšana, kuras pamatā ir automatizēta apstrāde, tostarp profilēšana, un ar kuru pamato lēmumus, kas fiziskai personai rada tiesiskās sekas vai līdzīgi būtiski ietekmē fizisko personu; b) 9.panta 1.punktā minēto īpašo kategoriju datu vai 10.pantā minēto personas datu par sodāmību un pārkāpumiem apstrāde plašā mērogā; vai c) publiski pieejamas zonas sistemātiska uzraudzība plašā mērogā.

Papildus iepriekš minētajam Datu valsts inspekcija skaidro, ka Regulas 35.pantā ir noteikts pārziņu pienākums noteiktos gadījumos izstrādāt novērtējumu par ietekmi uz datu aizsardzību. Novērtējums kalpo, gan kā rīks, kas ļauj pārzinim demonstrēt pārskatatbildību, gan arī ļauj pārzinim īstenot pašnovērtējumu attiecībā uz tā plānotajām personas datu apstrādes darbībām. Datu valsts inspekcija saskaņā ar Regulas 35.panta 4.punktu ir izstrādājusi sarakstu ar apstrādes darbību veidiem, attiecībā uz kuriem ir jāveic datu aizsardzības ietekmes novērtējums[1]. Šādas sistēmas izmantošanas, kuras ietvaros tiks veikta personas datu apstrāde, t.sk. profilēšana, būtu tāda personas datu apstrāde, pirms kuras uzsākšanas būtu veicams novērtējums par ietekmi uz datu aizsardzību.

Ņemot vērā iepriekš minēto, ***Datu valsts inspekcija norāda, ka RSU pirms uzsākt veikt personas datu apstrādi, izmantojot Respondus Monitor platformu, bija jāizvērtē samērīgums pret personu privātumu, kā arī jāveic novērtējums par ietekmi uz datu aizsardzību, bet tas netika izdarīts un līdz ar to ir konstatējums, ka RSU nav ievērojusī Regulas prasības***.

[1] https://www.dvi.gov.lv/lv/wp-content/uploads/Saraksts-ar-tiem-apstr%C4%81des-darb%C4%ABbas-veidiem-attiec%C4%ABb%C4%81-uz-kuriem-ir-j%C4%81veic-nov%C4%93rt%C4%93jums-par-ietekmi-uz-datu-aizsardz%C4%ABbu-NIDA1.pdf)

4.2. Attiecībā uz RSU vēstulē norādīto, ka ne Respondus Monitor, ne RSU neveic personas profilēšanu, Datu valsts inspekcija informē, ka Regulas 4.panta 4.punkts noteic, ka "profilēšana" ir jebkura veida automatizēta personas datu apstrāde, kas izpaužas kā personas datu izmantošana nolūkā izvērtēt konkrētus ar fizisku personu saistītus personiskus aspektus, jo īpaši analizēt vai prognozēt aspektus saistībā ar minētās fiziskās personas sniegumu darbā, ekonomisko situāciju, veselību, personīgām vēlmēm, interesēm, uzticamību, uzvedību, atrašanās vietu vai pārvietošanos. Darba grupas 2017.gada 3.oktobra pamatnostādnēs "Pamatnostādnes par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem" minēts, ka profilēšana sastāv no trim elementiem:

- apstrādes formai ir jābūt automatizētai;
- apstrāde veicama ar personas datiem un
- profilēšanas mērķim jābūt fiziskas personas personisko aspektu izvērtēšana.

Regulas 4.panta 4.punkts attiecas uz "jebkura veida automatizētu apstrādi", nevis "tikai" automatizētu apstrādi (uz ko atsaucas 22.pantā). Profilēšanai jāietver jebkāda veida automatizēta apstrāde, lai gan cilvēka iesaiste ne vienmēr nozīmē šīs darbības esību ārpus definīcijas.

Regulas profilēšanas definīcija ir ietekmējusies no Eiropas Padomes Ieteikumā CM/Rec (2010)13 (Ieteikums) sniegtās definīcijas, bet definīcijas nav identiskas, jo Ieteikumā ir izslēgta apstrāde, kas netver secinājumus. Tomēr ieteikumā sniegts noderīgs paskaidrojums, ka profilēšana var ietvert trīs atšķirīgus posmus:

- datu vākšana;
- automatizēta analīze nolūkā identificēt korelācijas;
- korelācijas piemērošana personai, lai noteiktu esošās vai turpmākās uzvedības pazīmes.

Līdz ar to, programma Respondus Monitor ir rīks, ar kā palīdzību ir iespējams veikt profilēšanu, nolūkā izvērtēt aizdomīgu studentu uzvedību pārbaudījumu laikā. Par to liecina arī Respondus, Inc tīmekļa vietnē https://web.respondus.com/he/monitor/ *(uzklikšķinot uz "Monitor AI is the most advanced artificial intelligence system for automated proctoring")* pieejama informācija (sk. šīs vēstules 1.punktu).

Regulas 60.apsvērums noteic, ka godprātīgas un pārredzamas apstrādes principi prasa to, ka datu subjekts ir informēts par apstrādes darbības esamību un tās nolūkiem. Pārzinim būtu jāsniedz datu subjektam jebkāda papildu informāciju, kas vajadzīga, lai nodrošinātu godprātīgu un pārredzamu apstrādi, ņemot vērā konkrētos apstākļus un kontekstu, kādā personas dati tiek apstrādāti. Turklāt datu subjektam vajadzētu būt informētam par profilēšanu un šādas profilēšanas sekām. Piemēram, ja personas datus iegūti no datu subjekta, pārzinim jāsniedz datu subjektam visa Regulas 13.pantā minētā informācija. Minēto informāciju var sniegt apvienojumā ar standartizētām ikonām, lai viegli uztveramā, saprotamā un skaidri salasāmā veidā sniegtu jēgpilnu pārskatu par paredzēto apstrādi. Ja ikonas attēlo elektroniski, tām vajadzētu būt mašīnlasāmām. Tas nozīmē, ka Jums būtu jāsniedz datu subjektiem visa Regulas 13.pantā noteiktā informācija.

Ievērojot minēto, Datu valsts inspekcija nekonstatē, ka šāda informācija tiek sniegta studentiem.

[5] RSU vēstulē minēts, ka RSU ieskatā virkne Datu valsts inspekcijas vēstulē uzdoto jautājumu saistībā ar Respondus Monitor platformām būtu adresējami šo platformas uzturētājiem, jo RSU, kā platformas lietotājas (balstoties uz licenci), rīcībā nav un nevar būt tik padziļināta informācija par katru no uzdotajiem jautājumiem.

Datu valsts inspekcija konstatē, ka Respondus, Inc tīmekļa vietnē https://web.respondus.com/data-processing/ ir pieejams "Data Processing Agreement" *(spēkā no 2018.gada 2.oktobra)*, kurā minēts, ka šis datu apstrādes līgums ("DPA") ir daļa no licences līguma starp Respondus, Inc. un licenciātu par licenciāta piekļuvi Respondus, Inc pakalpojumiem un to izmantošanu un ar to saistīto tehnisko atbalstu licenciātam. Šis datu apstrādes līgums atspoguļo pušu vienošanos attiecībā uz personas datu apstrādi un drošību [...].

Ievērojot minēto, Datu valsts inspekcija paskaidro, ka saskaņā ar Regulas 4.panta 7) apakšpunktu, par personas datu apstrādes atbilstību Regulai ir atbildīgs pārzinis (RSU).

Saskaņā ar Regulas 4.panta 8) apakšpunktu apstrādātājs ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura pārziņa vārdā apstrādā personas datus.

Darba grupas atzinumā 1/2010 "Par "personas datu apstrādātāja" un "apstrādātāja" jēdzienu" norādīts, ka "personas datu apstrādātāja" (turpmāk - pēc Regulas definējuma "pārziņa") jēdzienam un tā mijiedarbībai ar "apstrādātāja" jēdzienu ir principāla nozīme Direktīvas 95/46/EK piemērošanā, jo tie nosaka, kuras personas atbild par datu aizsardzības noteikumu ievērošanu, un kā datu subjekti praktiski var īstenot savas tiesības.

Tas nozīmē, ka personas datu apstrādātāja jēdziena galvenais uzdevums ir noteikt, kuras personas atbild par datu aizsardzības noteikumu ievērošanu, un kā datu subjekti var praktiski īstenot savas tiesības. Tātad — atbildības piešķiršana.

Tāpat Darba grupas atzinumā 1/2010 minēts, ka svarīgākais apstrādātāja definīcijas aspekts ir noteikums, ka apstrādātājs rīkojas "..pārziņa interesēs ..". Rīkoties kāda interesēs nozīmē apmierināt kāda intereses, un tas sasaucas ar juridisko jēdzienu "deleģēšana". Datu aizsardzības tiesību aktu gadījumā apstrādātāja uzdevums ir izpildīt pārziņa norādījumus vismaz attiecībā uz datu apstrādes nolūku un uz apstrādes līdzekļu pamatelementiem.

Raugoties no šāda viedokļa, apstrādātāja veikto datu apstrādes darbību likumību nosaka pārziņa piešķirtās pilnvaras. Apstrādātājs, kas pārsniedz piešķirtās pilnvaras un iegūst būtisku lomu datu apstrādes nolūku vai līdzekļu pamatelementu noteikšanā, ir drīzāk pārzinis, nevis apstrādātājs.

Regulas 28.panta 1.punkts paredz, ka gadījumos, kad apstrāde ir jāveic pārziņa vārdā, pārzinis izmanto tikai tādus apstrādātājus, kas sniedz pietiekamas garantijas, ka tiks īstenoti atbilstoši tehniskie un organizatoriskie pasākumi tādā veidā, ka apstrādē tiks ievērotas šīs regulas prasības un tiks nodrošināta datu subjekta tiesību aizsardzība.

Saskaņā ar Regulas 28.panta 3.punktu apstrādi, ko veic apstrādātājs, reglamentē ar līgumu vai ar citu juridisku aktu saskaņā ar Savienības vai dalībvalsts tiesību aktiem, kas ir saistošs apstrādātājam un pārzinim un kurā norāda līguma priekšmetu un apstrādes ilgumu, apstrādes raksturu un nolūku, personas datu veidu un datu subjektu kategorijas un pārziņa pienākumus un tiesības. Minētajā pantā arī ir iekļautas minimālās prasības apstrādātājam.

Ievērojot iepriekš minēto, Datu valsts inspekcija konstatē, ka RSU un Respondus, Inc situācijā, līguma noteikumus izstrādāja un piedāvāja Respondus, Inc, savukārt RSU kā pārzinis nevarēja tos ietekmēt. Vēršam uzmanību uz Darba grupas atzinumā 1/2010 minēto, ka, lai gan līgumattiecībās ar maziem pārziņiem lieliem pakalpojumu sniedzējiem ir lielākas iespējas diktēt savus noteikumus, tas nenozīmē, ka pārzinis var piekrist līguma noteikumiem un nosacījumiem, kas neatbilst datu aizsardzības tiesību aktu prasībām. Tāpat, Datu valsts inspekcija vērš uzmanību, ka, ievērojot Regulas 5.panta 2.punktā noteikto pārskatatbildības principu, tieši pārzinim (RSU) ir pienākums nodrošināt tādu personas datu apstrādes procesu, kas ļauj pierādīt, ka pārziņa veiktā personas datu apstrāde ir atbilstoša datu aizsardzības normatīvā regulējuma prasībām.

Ievērojot minēto, Datu valsts inspekcija konstatē, ka šobrīd RSU un Respondus, Inc attiecības nav noregulētas atbilstoši Regulas prasībām, kā arī RSU šobrīd nenodrošina Regulas 5.panta 2.punkta prasības.

Ņemot vērā iepriekš minēto, Datu valsts inspekcija konstatē, ka:

1. RSU veic biometrisko datu apstrādi, kas tiek uzskatīta par īpašu kategoriju personas datu apstrādi;
2. RSU iegūstot piekrišanu no studentiem, nav pilnvērtīgi ievērojusi Regulas prasības piekrišanas saņemšanai. Proti, ir konstatējams, ka RSU iegūstot piekrišanu, nepietiekami informē studentus par viņu personas datu apstrādi;
3. RSU veiktajā personas datu apstrādē, izmantojot Respondus Monitor platformu, ir nepietiekama personas datu apstrādes pārredzamības principa nodrošināšana un informācijas trūkums;
4. RSU nav izvērtējusi samērīgumu pret personu privātumu, kā arī nav veikusi

novērtējumu par ietekmi uz datu aizsardzību;

5. RSU nesniedz studentiem informāciju par profilēšanu un šādas profilēšanas sekām;

6. RSU un Respondus, Inc attiecības nav noregulētas atbilstoši Regulas prasībām, kā arī RSU šobrīd nenodrošina Regulas 5.panta 2.punkta prasības.

Ņemot vērā minēto un, pamatojoties uz Regulas 5.panta 1.punkta a) apakšpunktu, 12.panta 1.punktu, 58.panta 2.punkta d) apakšpunktu, Fizisko personu datu apstrādes likuma 23.pantu, Administratīvā procesa likuma (turpmāk – APL) 63.panta pirmās daļas 2.punktu, Datu valsts inspekcija nolemj uzlikt par pienākumu RSU līdz **2020.gada 20.jūlijam** veikt sekojošus pasākumus:

1. Nodrošināt pārredzamības principa ievērošanu, iegūstot personas datus no studentiem, t.sk. sniegt studentiem informāciju par profilēšanu un šādas profilēšanas sekām;

2. Nodrošināt Regulas 4.panta 11.punktam un 7.pantam atbilstošas piekrišanas iegūšanu no studentiem, ņemot vērā arī to, ka tiek apstrādāti arī īpašu kategoriju dati;

3. Veikt personas datu apstrādes, izmantojot Respondus Monitor platformu, samērīguma pret personu privātumu izvērtējumu;

4. Veikt novērtējumu par ietekmi uz datu aizsardzību;

5. Atbilstoši Regulas 28.pantam noregulēt RSU un Respondus, Inc. Savstarpējās attiecības.

Pamatojoties uz Fizisko personu datu apstrādes likuma 5.panta pirmās daļas 6.punktu un Regulas 58.panta 1.punkta a) apakšpunktu, paziņot Datu valsts inspekcijai par iepriekš minēto pienākumu izpildi rakstiski līdz **2020.gada 22.jūlijam** (pēdējā diena atbildes nosūtīšanai).

Datu valsts inspekcija savā darbībā īsteno principu "Konsultē vispirms"[2], kas paredz, ka Datu valsts inspekcijas darbībai primāri ir preventīva, nevis sodīšanas funkcija, līdz ar to, tās primārie uzdevumi ir efektīva fizisko personu datu aizsardzība (norādījumu par pārziņa veiktajā personas datu apstrādē konstatētajām nepilnībām un ierosinājumu sniegšana to novēršanai) un nelikumīgas personas datu apstrādes gadījumā nepieciešamo darbību veikšana ar mērķi pēc iespējas ātrāk pārtraukt to, tādā veidā mazinot datu subjektam radīto kaitējumu.

Regulas 58.panta 2.punkta b) apakšpunkts paredz Datu valsts inspekcijas pilnvaras izteikt rājienu pārzinim vai apstrādātājam, ja ar apstrādes darbībām ir tikuši pārkāpti šīs regulas noteikumi.

Pamatojoties uz iepriekš minēto, ņemot vērā pārkāpuma būtību, smagumu un to, kādu kategoriju personas datus ietekmējis pārkāpums, RSU sadarbības pakāpi ar Datu valsts inspekciju, Datu valsts inspekcija, pamatojoties uz Regulas 58.panta 2.punkta b) apakšpunktu, ***izsaka rājienu RSU un aicina RSU turpmākā darbībā, veicot personas datu apstrādi, ievērot šajā vēstulē minētas un citas Regulas un Fizisko personu datu apstrādes likuma prasības, izvērtēt dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisku personu tiesībām un brīvībām, ņemot vērā datu apstrādes raksturu, apmēru, kontekstu, nolūkus un veiktos tehniskos un organizatoriskos pasākumus, lai aizsargātu personas datus un novērstu to iespējamu nelikumīgu apstrādi, kā arī novērst neatbilstības, ja tādas ir, nodrošinot tiesisku personas datu apstrādi un aizsardzību.***

Lēmums tiks paziņots RSU, nosūtot to e-adreses informācijas sistēmā. *Saskaņā ar Fizisko personu datu apstrādes likuma 24.panta otro daļu, APL 76.panta pirmo un otro daļu, 79.panta pirmo daļu un Tieslietu padomes 2018.gada 5.marta lēmumu Nr.307 "Par tiesām, to darbības teritorijām un atrašanās vietām" šo lēmumu var apstrīdēt viena mēneša laikā no tā spēkā stāšanās dienas Administratīvās rajona tiesas attiecīgajā tiesu namā.*

[2] Datu valsts inspekcija 2017.gada 15.jūnijā parakstīja sadarbības memorandu par "Konsultē vispirms" principa iedzīvināšanu, veicinot valsts pārvaldes iestāžu uz klientu orientētu darbību

APL 70.panta pirmā daļa nosaka, ka, ja ārējā normatīvajā aktā vai pašā administratīvajā aktā nav noteikts citādi, administratīvais akts stājas spēkā ar brīdi, kad tas paziņots adresātam. Saskaņā ar APL 70.panta pirmo un otro daļu un Paziņošanas likuma 9.panta $1.^{1}$ daļu administratīvais akts uzskatāms par paziņotu otrajā darba dienā pēc tā nosūtīšanas.

Direktore J.Macuka

[..]

IZRAKSTS PAREIZS