SENĀTA LĒMUMS

RTU Senāta 2018. gada 28. septembra Senāta sēde (protokola Nr. 622)

Par Rīgas Tehniskās universitātes fizisko personu datu aizsardzības politikas apstiprināšanu jaunā redakcijā

Ņemot vērā Eiropas parlamenta un padomes 2016. gada 27. aprīļa regulu (ES) 2016/679 "Par fizisku personu datu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti", Senāts nolemj:

1. apstiprināt Rīgas Tehniskās universitātes fizisko personu datu aizsardzības politiku (turpmāk – Politika) jaunā redakcijā.
2. atzīt par spēku zaudējušu Senāta 2018.gada 21.maija lēmumu (protokola Nr. 620) "Par Rīgas Tehniskās universitātes fizisku personu datu aizsardzības politikas apstiprināšanu".

Rīgas Tehniskās universitātes fizisko personu datu aizsardzības politika

Izdota saskaņā ar Valsts pārvaldes iekārtas likuma 72. panta pirmās daļas 2. punktu un, ievērojot Augstskolu likuma 15.panta pirmo daļu

I. Vispārīgie jautājumi

1. Rīgas Tehniskās universitātes (turpmāk – RTU) fizisko personu datu aizsardzības politika (turpmāk – Politika) nosaka fizisko personu datu vākšanas, uzglabāšanas un apstrādāšanas pamatnostādnes, kas nodrošina fizisko personu datu aizsardzību, ieviešot un uzturot pietiekamu pasākumu kopumu potenciālā vai radītā kaitējuma mazināšanai vai novēršanai, un piemērojamo fizisko personu datu aizsardzības tiesību aktu, tostarp 2016. gada 27. aprīļa regulas (ES) 2016/679 "Par fizisku personu datu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti" ievērošanu.
2. Politika piemērojama RTU personālam, studentiem un citām pilnvarotām trešajām personām, kurām ir pieeja jebkuriem RTU fizisko personu datiem, ievērojot RTU informācijas un komunikācijas tehnoloģiju sistēmu drošības politiku un citus saistītos iekšējos normatīvos aktus, kas sniedz norādījumus par fizisko personu datu pareizu apstrādi.
3. Politika attiecināma uz jebkāda veida informāciju, kas ietver RTU uzglabātos (datorsistēmās, mobilajās ierīcēs, tālruņos, papīra ierakstos u.tml.), rakstītos, mutiski izteiktos un elektroniskos fizisko personu datus.

II. Politikā lietotie termini

4. Fizisko personu dati (turpmāk – personas dati) – ir jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu; identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem;

5. Īpašu kategoriju personas dati – sensitīvi personas dati, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, un ģenētisko datu, biometrisko datu, lai veiktu fiziskas personas unikālu identifikāciju, veselības datu vai datu par fiziskas personas dzimumdzīvi vai seksuālo orientāciju;
6. Apstrāde – jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana;
7. RTU personāls – personas, kurām ar RTU noslēgts darba līgums uz nenoteiktu vai noteiktu laiku, uzņēmuma, autortiesību līgums vai līgums par brīvprātīgā darbu vai praksi;
8. Datu subjekts – identificēta vai identificējama fiziska persona;
9. Pārzinis – RTU, kas nosaka personas datu apstrādes nolūkus un līdzekļus;
10. Apstrādātājs – fiziska (tostarp RTU personāls) vai juridiska persona, publiska iestāde (tostarp RTU), aģentūra vai cita struktūra, kura pārziņa vārdā apstrādā personas datus;
11. 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;
12. Datu aizsardzības speciālists – pārziņa iecelts speciālists, kuram ir speciālas zināšanas datu aizsardzības tiesību un prakses jomā un kurš spēj informēt un konsultēt pārzini vai apstrādātāju un darbiniekus, kuri veic apstrādi, par viņu pienākumiem saskaņā ar datu aizsardzību regulējošajiem normatīvajiem aktiem; uzraudzīt, vai tiek ievēroti datu aizsardzību regulējošie normatīvie akti un pārziņa vai apstrādātāja politika saistībā ar personas datu aizsardzību, tostarp pienākumu sadali, apstrādes darbībās iesaistīto darbinieku informēšanu un apmācību, un ar to saistītajām revīzijām; pēc pieprasījuma sniegt padomus attiecībā uz novērtējumu par ietekmi uz datu aizsardzību un pārraudzīt tā īstenošanu; sadarboties ar Datu valsts inspekciju; būt par Datu valsts inspekcijas kontaktpunktu jautājumos, kas saistīti ar apstrādi un attiecīgā gadījumā konsultēt par jebkuru citu jautājumu;
13. Privātuma paziņojums – paziņojums datu subjektam par konfidencialitāti, lai sniegtu datu subjektam ieskatu par to, kā apstrādātājs vāc, izmanto, uzglabā un kopīgo datu subjekta personas datus (norādot personas datu apstrādes nolūkus un likumīgo pamatu), kā arī, kādus pasākumus apstrādātājs veic, lai aizsargātu datu subjekta personas datus, papildus datu subjektam darot zināmu, ka datu subjekts var lūgt: piekļūt apstrādātāja rīcībā esošajiem personas datiem par datu subjektu vai mainīt tos; atsaukt apstrādātājam iepriekš sniegto piekrišanu; nesūtīt datu subjektam noteiktus paziņojumus un atbildēt uz jautājumiem, kas datu subjektam var rasties saistībā ar apstrādātāja privātuma praksi;
14. Pseidonimizācija – personas datu apstrāde, ko veic tādā veidā, lai personas datus vairs nav iespējams saistīt ar konkrētu datu subjektu bez papildu informācijas izmantošanas, ar noteikumu, ka šāda papildu informācija tiek turēta atsevišķi un tai piemēro tehniskus un organizatoriskus pasākumus, lai nodrošinātu, ka personas dati netiek saistīti ar identificētu vai identificējamu fizisku personu;
15. Pikšķerēšana – arī fišings *(angļu: phishing)* datorzinātnē ir nelikumīgs veids, kurā mēģina ar viltu iegūt no interneta lietotāja slepenu informāciju, piemēram, lietotāju vārdus, paroles, kredītkaršu numurus.

III. Personas datu aizsardzības principi

16. Apstrādājot personas datus jāievēro šādi personas datu aizsardzības principi:
    16.1. personas datu likumīga, taisnīga un pārredzama apstrāde;
    16.2. personas datu vākšana tikai konkrētiem, skaidriem un likumīgiem nolūkiem un to apstrāde tādā veidā, lai tā būtu saderīga ar šiem likumīgajiem mērķiem;
    16.3. tikai tādu personas datu apstrāde, kura ir atbilstoša un nepieciešama attiecīgajiem mērķiem;
    16.4. precīzu un atjauninātu personas datu uzturēšana un pasākumu veikšana, lai nodrošinātu, ka neatbilstoši personas dati tiek nekavējoties dzēsti vai laboti;
    16.5. personas datu saglabāšana tādā formā, kas ļauj identificēt datu subjektus ne ilgāk kā tas ir nepieciešams nolūkiem, kādiem dati tiek apstrādāti;
    16.6. atbilstošu tehnisko un organizatorisko pasākumu veikšana, lai nodrošinātu to, ka personas dati tiek glabāti droši un aizsargāti pret neatļautu vai nelikumīgu apstrādi, kā arī pret nejaušu nozaudēšanu, iznīcināšanu vai bojājumiem.
17. RTU ir arī atbildīga par to, lai pierādītu atbilstību iepriekš minētajiem datu aizsardzības principiem.

IV. Personas datu apstrādes pamats

18. Saistībā ar jebkuru apstrādes darbību, kas ietver personas datus, pirms apstrādes uzsākšanas, un pēc tam regulāri, kamēr tā turpināsies, jāpārliecinās, ka:
    18.1. konkrētās apstrādes darbības mērķi ir pārskatīti un ir piemeklēts vispiemērotākais likumīgais pamats šai apstrādei, t.i.:
        18.1.1. ka datu subjekts ir piekritis apstrādei;
        18.1.2. apstrāde ir nepieciešama līguma, kura līgumslēdzēja puse ir datu subjekts, izpildei vai, lai veiktu pasākumus pēc datu subjekta pieprasījuma pirms līguma noslēgšanas;
        18.1.3. apstrāde ir nepieciešama, lai izpildītu uz RTU attiecināmu juridisku pienākumu;
        18.1.4. apstrāde ir nepieciešama datu subjekta vai citas fiziskas personas būtisko interešu (tostarp fiziskās veselības vai dzīvības) aizsardzībai;
        18.1.5. apstrāde ir vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs, vai, īstenojot RTU normatīvajos aktos noteiktās saistības;
        18.1.6. apstrāde ir nepieciešama RTU vai trešās personas likumīgo interešu ievērošanai, izņemot gadījumus, kad datu subjekta intereses vai pamattiesības un pamatbrīvības, kurām nepieciešama personas datu aizsardzība, ir svarīgākas par šādām interesēm.
    18.2. apstrāde ir nepieciešama attiecīgajam likumīgajam nolūkam (gadījumos, kad apstrāde ir balstīta tikai uz piekrišanu, un nav cita pamatojuma apstrādei);
    18.3. tiek dokumentēts likumīgais pamats, kas tiek piemērots konkrētai apstrādei, lai apliecinātu atbilstību datu aizsardzības principiem;
    18.4. datu subjektam pastāv iespēja iepazīties ar privātuma paziņojumu (Politikas 10.punkts);
    18.5. tiek noteikts un dokumentēts likumīgs nosacījums, lai apstrādātu īpašās kategorijas personas datus.

V. Īpašu kategoriju personas dati

19. Īpašu kategoriju jeb sensitīvus personas datus var apstrādāt, ja:

    19.1. pastāv likumīgs pamats, un
    19.2. ir piemērojams viens no īpašajiem nosacījumiem, lai apstrādātu sensitīvus personas datus:
        19.2.1. datu subjekts ir devis nepārprotamu piekrišanu šo personas datu apstrādei;
        19.2.2. apstrāde ir nepieciešama RTU vai datu subjekta darba tiesisko attiecību īstenošanai;
        19.2.3. apstrāde ir nepieciešama, lai aizsargātu datu subjekta vai citas fiziskas personas svarīgas (tostarp ar veselību un dzīvību saistītas) intereses, un datu subjekts fiziski vai tiesiski nespēj dot piekrišanu;
        19.2.4. apstrāde attiecas uz personas datiem, kurus datu subjekts apzināti ir publiskojis;
        19.2.5. apstrāde ir vajadzīga, lai celtu, īstenotu vai aizstāvētu likumīgas prasības, vai ikreiz, kad tiesas pilda savus uzdevumus; vai
        19.2.6. apstrāde ir nepieciešama būtisku sabiedrības interešu dēļ, kas ir samērīgas izvirzītajam mērķim, ievēro tiesību uz datu aizsardzību būtību un paredz piemērotus un konkrētus pasākumus datu subjekta pamattiesību un interešu aizsardzībai.

VI. Datu privātuma ietekmes novērtējums

20. Ja apstrāde var radīt lielu risku fizisko personu tiesībām un brīvībām (piemēram, ja RTU plāno izmantot jaunu tehnoloģisku veidu, kā apstrādāt personu datus), pirms apstrādes uzsākšanas, jāveic datu privātuma ietekmes novērtējums, lai novērtētu:

    20.1. vai apstrāde ir nepieciešama un proporcionāla izvirzītajam apstrādes mērķim;
    20.2. vai pastāv risks fizisko personu tiesībām un brīvībām;
    20.3. kādus papildu drošības pasākumus var ieviest, lai novērstu riskus un aizsargātu personas datus.

VII. Dokumentācija

21. Personas datu apstrāde reģistrējama RTU personas datu apstrādes reģistrā. Katrai personas datu apstrādei ir identificēts nolūks, apstrādes juridiskais pamats, datu subjektu kategorijas, saņēmēju kategorijas, paredzētie personu datu glabāšanas termiņi, kā arī atbildīgā struktūrvienība, kura ir atbildīga gan par personas datu apstrādes procesu, gan ar to saistītās informācijas aktualizāciju reģistrā.
22. RTU regulāri atjauno ar personu datu apstrādi saistīto dokumentāciju, kas var ietvert:
    22.1. informācijas auditu veikšanu, lai noskaidrotu, kādus personas datus glabā RTU sistēmās;
    22.2. aptaujas lapu izplatīšanu un sarunas ar darbiniekiem visā RTU, lai iegūtu pilnīgāku priekšstatu par apstrādes darbībām; un
    22.3. Politikas, procedūru, līgumu pārskatīšanu, lai nodrošinātu datu drošību.

VIII. Privātuma paziņojumi

23. Administratīvais departaments nodrošina vispārīga privātuma paziņojuma publicēšanu RTU mājaslapā, kā arī informāciju par to, kur datu subjekts var uzzināt par savu datu apstrādi un to likumīgo pamatu.
24. Gadījumos, kad tiek uzsākta personu datu apstrāde, RTU nodrošina privātuma paziņojuma sniegšanu datu subjektam īsā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru valodu.

IX. Datu subjekta tiesības

25. Datu subjektiem ir šādas tiesības attiecībā uz viņa personas datiem:
    25.1. būt informētam par to, kā, kāpēc un uz kāda pamata tiek apstrādāti dati;
    25.2. iegūt apstiprinājumu, vai datu subjekta dati tiek apstrādāti, un apstiprinājuma gadījumā iegūt piekļuvi tiem, iesniedzot atbilstošu pieprasījumu;
    25.3. panākt datu labošanu, ja tie ir neprecīzi vai nepilnīgi;
    25.4. panākt, lai dati tiktu dzēsti, ja tie vairs nav vajadzīgi nolūkam, kādam tie sākotnēji tika savākti un apstrādāti, vai, ja vairs nepastāv likumīgs šīs apstrādes pamatojums (to sauc arī par "tiesībām tikt aizmirstam");
    25.5. panākt personas datu apstrādes ierobežošanu, ja informācijas precizitāte tiek apstrīdēta, vai apstrāde ir nelikumīga (bet datu subjekts nevēlas, lai viņa dati tiktu dzēsti) vai arī, ja RTU vairs nav nepieciešami personas dati, bet datu subjekts pieprasa tos atstāt, lai aizstāvētu sevi tiesā;
    25.6. panākt personas datu apstrādes ierobežošanu uz laiku, ja datu subjekts uzskata, ka tie ir neprecīzi (un RTU veic datu precizitātes pārbaudi), vai, ja datu subjekts ir iebildis pret datu apstrādi (un RTU veic izvērtējumu, vai RTU likumīgais pamatojums prevalē pār datu subjekta interesēm).
26. RTU privātuma paziņojumos tiek sniegta informācija par to, ka datu subjekts ir tiesīgs sazināties ar RTU datu aizsardzības speciālistu par savu tiesību izmantošanas iespējām.

X. Individuālie pienākumi

27. Datu subjektam ir pienākums informēt RTU par jebkurām izmaiņām savos personas datos, kas nodoti RTU.
28. No apstrādātāja, kurš, pildot savus amata pienākumus, var piekļūt RTU personāla, studentu un citu datu subjektu personas datiem, RTU sagaida godprātīgu attieksmi pret šiem datiem, lai izpildītu uzņemtās saistības nodrošināt personas datu konfidencialitāti un integritāti.

29. Apstrādātājs, kuram ir piekļuve RTU personas datiem:
    29.1. piekļūst tikai tiem personas datiem, kuriem apstrādātājam ir tiesības piekļūt, un tikai atbilstošā apjomā un atļautajam mērķim (nav atļauts bezmērķīgi interesēties par datiem);
    29.2. ļauj trešajām personām piekļūt personas datiem tikai tad, ja viņām ir dota atbilstoša atļauja;
    29.3. aizsargā personas datus (tai skaitā, ievērojot RTU informācijas un komunikācijas tehnoloģiju sistēmu drošības politiku un ar to saistītos noteikumus par piekļuvi telpām, piekļuvi datoram, paroļu aizsardzību un drošu failu glabāšanu un iznīcināšanu, kā arī ievēro citus piesardzības pasākumus, apstrādājot personas datus);
    29.4. nenes prom (uz mājām) datus vai ierīces, kurās ir personas dati (vai kuras var izmantot, lai piekļūtu tiem), ja vien nav veikti atbilstoši drošības pasākumi (piemēram, pseidonimizācija, šifrēšana ar atbilstošas paroles aizsardzību), lai nodrošinātu informācijas konfidencialitāti ierīcē.
30. Pārzinis, apstrādātājs vai datu subjekts informē RTU datu aizsardzības speciālistu, ja ir noticis (vai notiek vai ar ļoti lielu varbūtību varētu notikt) viens no šādiem gadījumiem:
    30.1. notiek personas datu apstrāde bez likumīga pamatojuma, vai attiecībā uz sensitīviem personas datiem, netiek izpildīts vismaz viens no Politikas 12.punktā minētajiem nosacījumiem;
    30.2. tiek nodrošināta piekļuve personas datiem bez atbilstošas autorizācijas;
    30.3. personas dati netiek droši glabāti vai dzēsti;
    30.4. neveicot atbilstošus drošības pasākumus no RTU tiek iznesti personas dati vai ierīces, kas satur personas datus (vai kuras var izmantot, lai tiem piekļūtu);
31. notiek jebkurš cits šo iekšējo noteikumu, vai jebkurš 16.punktā noteiktais datu aizsardzības principa pārkāpums.

XI. Informācijas drošība

32. RTU izmanto atbilstošus tehniskos un organizatoriskos pasākumus saskaņā ar RTU informācijas un komunikācijas tehnoloģiju sistēmu drošības politiku un citiem saistītajiem iekšējiem normatīvajiem aktiem, lai saglabātu personas datu drošību, un, jo īpaši, lai aizsargātu tos pret neatļautu vai nelikumīgu datu apstrādi un/vai nejaušu nozaudēšanu, iznīcināšanu vai bojāšanu. Tie var ietvert:
    32.1. pārliecību, ka, kur iespējams, personas dati ir pseidonimizēti vai šifrēti;
    32.2. pārliecību par apstrādes sistēmās esošo datu konfidencialitāti, integritāti, pieejamību un noturību;
    32.3. pārliecību, ka fiziska vai tehniska rakstura incidenta gadījumā savlaicīgi var atjaunot personas datus un nodrošināt piekļuvi tiem; un
    32.4. ir iedibināti procesi, kas regulāri pārbauda un novērtē tehnisko un organizatorisko pasākumu efektivitāti, lai nodrošinātu datu apstrādes drošību.
33. Gadījumā, ja RTU izmanto trešās personas, lai apstrādātu personas datus savā vārdā, ir nepieciešams līgumos iestrādāt papildu drošības pasākumus attiecībā uz datu konfidencialitāti un integritāti. Jo īpaši līgumos ar trešajām personām jānodrošina, to, ka:
    33.1. trešā persona var rīkoties tikai saskaņā ar RTU rakstiskām instrukcijām;
    33.2. trešā persona, kas apstrādā datus, ir uzticama;
    33.3. tiek veikti atbilstoši pasākumi, lai nodrošinātu apstrādes drošību;
    33.4. apakšuzņēmēji ir iesaistīti tikai ar RTU iepriekšēju piekrišanu un saskaņā ar rakstisku līgumu;

33.5. trešā persona palīdzēs RTU nodrošināt datu subjekta tiesības personas datu jomā;
33.6. trešā persona palīdzēs RTU pildīt savas saistības attiecībā uz datu apstrādes drošību, paziņojumiem par datu pārkāpumiem un datu aizsardzības ietekmes novērtējumu;
33.7. izbeidzoties līgumam, trešā persona izdzēsīs vai nodos RTU visus tai uz līguma pamata nodotos personas datus;
33.8. trešā persona nodrošinās RTU ar informāciju, kura ir nepieciešama, lai nodrošinātu datu aizsardzības pienākumu izpildi.

34. Pirms tiek noslēgts jauns līgums (vai esošais līgums tiek grozīts), kas ietver trešās personas veiktu personas datu apstrādi, par līguma slēgšanu atbildīgais darbinieks saņem akceptu no RTU datu aizsardzības speciālista.

XII. Personas datu glabāšana

35. Personas dati un sensitīvie personas dati tiks droši uzglabāti saskaņā ar RTU informācijas un komunikācijas tehnoloģiju sistēmu drošības politiku.
36. Personas datus un sensitīvus personas datus nedrīkst uzglabāt ilgāk, kā nepieciešams atbilstošam nolūkam. Datu saglabāšanas ilgums atkarīgs no apstākļiem, tostarp nolūkiem, kādēļ personas dati tika iegūti.
37. Personas dati un sensitīvie personas dati, kas vairs nav nepieciešami, tiks neatgriezeniski izdzēsti no RTU informācijas sistēmām. Dati no rezerves kopijām tiks izdzēsti tiklīdz beigsies rezerves kopijas uzglabāšanas laiks.

XIII. Datu aizsardzības pārkāpumi

38. Datu aizsardzības pārkāpums var būt dažāds, piemēram:
38.1. datu vai aprīkojuma, uz kura tiek glabāti personas dati, zudums vai tā zādzība;
38.2. nesankcionēta piekļuve personas datiem;
38.3. iekārtas vai sistēmu (tostarp aparatūras un programmatūras) kļūdas rezultātā esošais datu zudums;
38.4. cilvēka kļūdas rezultāts, piemēram, nejauša datu dzēšana vai izmaiņu veikšana;
38.5. neparedzēti apstākļi, piemēram, ugunsgrēks vai plūdi;
38.6. apzināti uzbrukumi IT sistēmām, piemēram, sistēmu uzlaušana, vīrusu vai pikšķerēšanas veida uzbrukumi.

39. Ja ir aizdomas, ka RTU rīcībā esošie personas dati ir jebkādā veidā apdraudēti, nekavējoties jāziņo RTU personu datu aizsardzības speciālistam.
40. RTU apņemas:
40.1. izpētīt visus ziņotos faktiskos vai iespējamos datu drošības pārkāpumus;
40.2. gadījumā, ja tas var apdraudēt personas tiesības un brīvības, bez vilcināšanās un, ja iespējams, 72 stundu laikā no brīža, kad ir kļuvis zināms par pārkāpumu, sniedz nepieciešamo informāciju par datu pārkāpumu Datu valsts inspekcijai;
40.3. informēt skartos indivīdus, ja datu zudums varētu radīt lielu risku viņu tiesībām un brīvībām, un, ja šāda paziņošana ir nepieciešama saskaņā ar normatīviem aktiem.

XIV. Starptautiskā datu nodošana

41. RTU var nodot personas datus ārpus Eiropas Ekonomikas zonas (kas ietver Eiropas Savienības (ES) un Islandes, Lihtenšteinas un Norvēģijas valstis) un uz citām valstīm, pamatojoties uz to, ka šajās valstīs noteiktās aizsardzības prasības ir atbilstošas ES prasībām vai ka organizācija, kas saņem informāciju, ir nodrošinājusi pietiekamas garantijas (piemēram, izmantojot saistošus uzņēmumu noteikumus vai standarta datu

aizsardzības klauzulas) vai arī, ja RTU iegūst attiecīgo datu subjektu nepārprotamu piekrišanu šādai datu nodošanai.

42. Apstrādātājam ir pienākums informēt datu subjektu par visiem paredzētajiem starptautiskiem personas datu nodošanas gadījumiem attiecīgā privātuma paziņojumā.

XV. Apmācība

43. RTU nodrošina RTU personāla atbilstošu apmācību datu aizsardzības jomā. Apstrādātājam (kuram nepieciešama regulāra piekļuve personas datiem, vai kurš ir atbildīgs par atbildes sniegšanu uz attiecīgajiem datu subjektu pieprasījumiem) RTU nodrošina papildu apmācību, lai palīdzētu apstrādātājam saprast savus pienākumus un to pareizu izpildi.

XVI. Noslēguma jautājumi

44. RTU attiecas pret personas datu aizsardzību ļoti nopietni. Neievērojot personu datu aizsardzību:
    44.1. tiek apdraudētas personas, kuru personas dati tiek apstrādāti;
    44.2. tiek palielināts risks radīt būtiskas civiltiesiskās un krimināltiesikās sankcijas apstrādātājam un pārzinim.
45. Ņemot vērā personas datu aizsardzības nozīmīgumu, prasību attiecībā uz personu datu aizsardzību neievērošana var izraisīt disciplinārus pasākumus saskaņā ar RTU iekšējiem noteikumiem, un šīs darbības, nopietna pārkāpuma rezultātā var novest pie darba līguma uzteikšanas. Ja persona, kas pārkāpj prasības attiecībā uz personu datu aizsardzību, nav RTU darbinieks, līgumu ar šo personu var izbeigt nekavējoties.
46. RTU datu aizsardzības speciālists ir atbildīgs par RTU un tās darbinieku informēšanu un konsultēšanu par fizisko personu datu aizsardzības pienākumiem, kā arī par RTU Politikas īstenošanas uzraudzību (e-pasts: datuaisardziba@rtu.lv, tālrunis: 67089833).
47. Kārtību, kādā RTU tiek organizēta personas datu apstrāde, aizsardzība nosaka rektora apstiprināti iekšējie normatīvie akti.

Senāta priekšsēdētāja E. Gaile-Sarkane

Sagatavoja Administratīvais departaments.