BANKU AUGSTSKOLA

PVN Reģ. Nr. LV 90000437699, K.Valdemāra ielā 161, Rīgā, LV-1013, tālr.67360133, fakss 67320620, e-pasts: info@ba.lv, http://www.ba.lv

APSTIPRINĀTS
Banku augstskolas
Senāta 22.05.2018. sēdē,
protokols Nr.6

Incidentu pārvaldības kārtība Banku augstskolā fizisko personu datu drošības jomā

Rīgā

Izdots saskaņā ar Augstskolu likuma 15.panta pirmo daļu un Banku augstskolas Satversmes 21.punktu

2018.gada 22.maijā Nr.1.5-2/12

I. Vispārīgie noteikumi

1. Incidentu pārvaldības kārtība Banku augstskolā fizisko personu datu drošības jomā (turpmāk – kārtība) nosaka rīcību, kāda veicama gadījumos, kad Banku augstskolā (turpmāk – augstskola) ir identificēta fizisko personu datu apstrāde, kas ir pretrunā Latvijas Republikā spēkā esošajiem ārējiem normatīvajiem aktiem un augstskolas iekšējiem normatīvajiem aktiem, kuri reglamentē fizisko personu datu apstrādi un to drošību.

2. Kārtība attiecas uz incidentiem un incidentu riskiem, kas ir notikuši vai var notikt, apstrādājot fizisko personu datus jebkurā no veidiem, kas ir minēti Latvijas Republikā normatīvajos aktos.

3. Kārtība nosaka nepieciešamo rīcību gadījumos, kad incidents vai incidenta risks ir radies no augstskolas personāla, praktikantu, kā arī pakalpojumu sniedzēju augstskolai rīcības neatkarīgu tehnisku apstākļu dēļ.

4. Kārtībā tiek lietotie šādi termini:

4.1. informācijas sistēmas – augstskolā izmantojamās elektroniskās informācijas sistēmas (tostarp videonovērošanas sistēma), kuras tiek izmantotas fizisko personu datu apstrādei;

4.2. incidents – pārkāpums attiecībā uz fizisko personu datu apstrādi, kas izpaužas kā normatīvo aktu prasībām neatbilstoša rīcība - personas datu:

4.2.1. izpaušana;

4.2.2. kopēšana;

4.2.3. iegūšana;

4.2.4. glabāšana;

4.2.5. ievadīšana informācijas sistēmā;

4.2.6. reģistrēšana;
4.2.7. pārveidošana;
4.2.8. pārraidīšana;
4.2.9. bloķēšana;
4.2.10. dzēšana.

II. Incidentu novēršana

5. Par incidentu pārraudzību un novēršanu attiecībā uz informācijas sistēmām augstskolā atbildīga ir tā persona, kura noteikta kā atbildīgā persona par augstskolas tehniskajiem resursiem - Informācijas tehnoloģiju daļas vadītājs (turpmāk – IT daļas vadītājs).

6. Par incidentu pārraudzību un novēršanu, apstrādājot personas datus, manuāli, tostarp, papīra formā, atbild ar augstskolas rektora rīkojumu norīkotas personas.

7. IT daļas vadītāja pienākumus ir informēt augstskolas personālu, praktikantus, kā arī pakalpojumu sniedzējus augstskolai par potenciālajiem incidentu riskiem informācijas sistēmās.

8. Ja datu drošības pārbaužu rezultātā tiek konstatēti potenciāli incidentu riski informācijas sistēmās, IT daļas vadītājs organizē attiecīgā incidenta riska novēršanu. Gadījumos, kad incidenta risks ir radies attiecīgās informācijas sistēmas izstrādātāja vai uzturētāja darbības, bezdarbības vai attiecīgās informācijas sistēmas tehnisku nepilnību rezultātā, IT daļas vadītājs informē par to attiecīgās informācijas sistēmas izstrādātāju vai uzturētāju (datu apstrādes operatoru) un vienojas ar to par termiņu, kurā tiek novērsti identificētie incidenta riski.

9. Augstskolas personāla, praktikantu, kā arī pakalpojumu sniedzēju augstskolai pienākums ir būt informētiem par visbiežāk sastopamajām pazīmēm, kas var liecināt par iespējamo informācijas sistēmas drošības pārkāpumu, kurš var izraisīt incidentus, tostarp, īpašu uzmanību vēršot uz šādām pazīmēm:

9.1. pretvīrusu programmatūras brīdinoši signāli informācijas sistēmas lietotāja datora inficēšanas gadījumā;

9.2. datņu ar nosaukumiem, kas satur neparastas zīmes, parādīšanās;

9.3. elektroniskā pasta vēstules no nepazīstamiem sūtītājiem, kuras nesatur loģiski saprotamu tekstu vai datnes.

III. Ziņošana par incidentu

10. Augstskolas personāls, praktikanti, kā arī pakalpojumu sniedzēji augstskolai, kuri konstatē incidentu, nekavējoties par to ziņo IT daļas vadītājam.

11. Ja incidents ir radies, apstrādājot datus ārpus informācijas sistēmām, incidentu konstatējušie augstskolas personāls, praktikanti, kā arī pakalpojumu sniedzēji augstskolai informē par to IT daļas vadītāju, kurš, ja nepieciešams, par to informē augstskolas rektoru.

12. IT daļas vadītājs veic visas nepieciešamās darbības incidenta pārtraukšanai, tā radīto seku novēršanai un līdzīgu incidentu novēršanai.

13. IT daļas vadītājs ziņo augstskolas rektoram un Datu valsts inspekcijai, ja ir konstatēts, ka incidenta rezultātā notikusi fizisko personu datu noplūde, un veic citas darbības, ja tas nepieciešams, informē fizisko personu datu subjektu saskaņā ar fizisko personu datu apstrādes un aizsardzības noteikumiem Banku augstskolā.

14. Ja incidenta rašanās ir saistīta ar krimināli sodāmu darbību, vienas dienas laikā no incidenta atklāšanas dienas IT daļas vadītājs informē augstskolas rektoru, kurš lemj par tiesībsargājošo iestāžu informēšanu par šo notikumu.

IV. Neatliekamo darbību veikšana

15. Konstatējot incidentu, augstskolas personāla, praktikantu, kā arī pakalpojumu sniedzēju augstskolai pienākums ir novērst vai apturēt to savas kompetences ietvaros.

16. Ja IT nodaļas vadītājs konstatē augstskolas informācijas resursa drošības pārkāpumu, viņš var veikt šādas darbības:

16.1. brīdināt par informācijas resursa neatbilstošo izmantošanu informācijas sistēmas lietotāju, kurš pārkāpj informācijas sistēmas izmantošanas noteikumus;

16.2. anulēt kārtības 16.1.apakšpunktā minētajam informācijas sistēmas lietotājam piekļuves tiesības attiecīgajai informācijas sistēmai;

16.3. veikt nepieciešamās darbības, lai ierobežotu piekļuvi informācijas resursa neatbilstošai izmantošanai.

16.4. pārbaudīt piekļuves tiesības visām augstskolas informācijas sistēmām;

16.5. informēt attiecīgās informācijas sistēmas izstrādātāja vai uzturētāja pārstāvi, ja incidents ir radies attiecīgās informācijas sistēmas uzturētāja darbības vai bezdarbības vai attiecīgās informācijas sistēmas tehnisku nepilnību rezultātā un uzdot tam saprātīgā termiņā novērst apstākļus, kuru dēļ ir radies incidents.

17. Ja augstskolas personāls, strādājot ar informācijas sistēmu, konstatē incidentu, kļūdas paziņojumu, darbinieka pienākums ir:

17.1. fiksēt kļūdas paziņojuma tekstu;

17.2. pierakstīt darbību secību, kuru rezultātā radās kļūdas situācija;

17.3. pārtraukt darbu ar informācijas sistēmu;

17.4. ziņot IT daļas vadītājam par konstatēto.

V. Turpmākā rīcība

18. Pēc incidenta informācijas sistēmās un tā radīto seku novēršanas IT daļas vadītājs veic incidenta riska analīzi.

19. Ja incidenta rezultātā ir konstatēts būtisks kaitējums fizisko personu datu subjekta ar

likumu aizsargātajām interesēm (piemēram, augstskolas personāla sensitīvo datu izpaušana), IT daļas vadītājs sadarbībā ar fizisko personu datu aizsardzības speciālistu vai atbildīgajām personām par datu drošību augstskolā divu nedēļu laikā pēc incidenta konstatēšanas sagatavo un iesniedz augstskolas rektoram ziņojumu, kurā ir ietverta šāda informācija:

19.1. incidenta apraksts;

19.2. apstākļi, kas veicinājuši incidenta rašanos;

19.3. par incidenta rašanos atbildīgie augstskolas personāls, praktikanti, kā arī pakalpojumu sniedzēji augstskolai;

19.4. veicamās darbības incidenta novēršanai;

19.5. incidenta radītais kaitējums;

19.6. veiktās un veicamās darbības, lai novērstu incidenta atkārtošanos.

20. Augstskolas rektors pēc iepazīšanās ar ziņojumu lemj par vienu vai vairākām šādām darbībām:

20.1. pieņemt informāciju zināšanai;

20.2. uzdot veikt nepieciešamos uzlabojumus, lai novērstu incidenta atkārtošanos (gadījumā, ja uzskata līdz ziņojuma iesniegšanai veiktos pasākumus par nepietiekamiem);

20.3. par nepieciešamību ierosināt disciplinārlietu;

20.4. par tiesībsargājošo iestāžu vai Datu valsts inspekcijas informēšanu;

20.5. par pretenzijas iesniegšanu attiecīgajam informācijas sistēmas izstrādātājam vai uzturētājam, ja pārkāpums radies tā darbības vai bezdarbības rezultātā vai informācijas sistēmas tehnisko nepilnību dēļ.