SIA "Biznesa augstskola Turība"
Vienotais reģistrācijas Nr.40003135880
Graudu ielā 68, Rīgā, LV-1058

V117
APSTIPRINĀTS
ar SIA "Biznesa augstskola Turība"
Valdes 08.05.2018. lēmumu Nr.21

PERSONAS DATU APSTRĀDES UZ AIZSARDZĪBAS POLITIKA

I. Vispārīgie jautājumi

1. SIA „Biznesa augstskola Turība" (turpmāk – BAT) personas datu apstrādes un aizsardzības politika nosaka personas datu apstrādes un aizsardzības sistēmas (turpmāk – Sistēma) ieviešanas un pārvaldības pamatnostādnes, kuru mērķis ir nodrošināt BAT veikto personas datu apstrādes darbību atbilstību Regulas prasībām, kā arī veikt organizatorisku pasākumu kopumu potenciālo risku vai radītā kaitējuma mazināšanai vai novēršanai.
2. Politika attiecas uz jebkurām BAT kā datu apstrādes pārziņa veiktajām datu apstrādes darbībām, kā arī iekšējo un ārējo informācijas un tehnisko resursu kopumu, kas ir izveidots, strādā un tiek uzturēts, lai vāktu, uzkrātu, apstrādātu, uzglabātu un izmantotu personas datus, kā arī citu informāciju.
3. Organizatoriskie pasākumi Sistēmas ieviešanai un pārvaldībai tiek veikti ievērojot samērīguma principu, kur ieviesto pasākumu izmaksas nepārsniedz potenciālā kaitējuma iestāšanās rezultātā nodarītos zaudējumus.

II. Politikā lietotie termini

4. Regula – Eiropas Parlamenta un Padomes regula Nr.2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula);
5. Personas dati - jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu ("datu subjektu"); 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;
6. Datu subjekts – šī dokumenta izpratnē BAT vispārējais un akadēmiskais personāls, studējošie, kursu klausītāji vai jebkura cita fiziska persona, kuras personas datus BAT apstrādā;
7. Datu 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;
8. Datu subjekta piekrišana - 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;
9. Personas datu aizsardzības pārkāpums (incidents) - ir drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem;
10. Par datu apstrādes un aizsardzības Sistēmu atbildīgā persona – BAT valdes norīkota persona, kura uzrauga un kontrolē personas datu apstrādes procesus;
11. IT Sistēma – ir iekšējo un ārējo informācijas un tehnisko resursu kopums, kas ir izveidots, strādā un tiek uzturēts, lai vāktu, uzkrātu, apstrādātu, uzglabātu un izmantotu informāciju, kura tiek pārvaldīta atbilstoši BAT informācijas un komunikācijas tehnoloģijas sistēmu drošības politikai;
12. IT Sistēmu drošības pārvaldnieks – BAT valdes norīkota persona, kura īsteno IT Sistēmu drošības pārvaldību BAT;

13. BAT struktūrvienība – BAT struktūrvienība, kura izveidota un darbojas uz BAT valdes apstiprināta nolikuma pamata;

III. Personas datu apstrādes pamatprincipi

14. BAT personas datu apstrādes un aizsardzības sistēma tiek veidota ievērojot šādus pamatprincipus:

14.1. likumīguma, godprātības un pārredzamības principu, kas nozīmē, ka personas dati tiek apstrādāti likumīgi, godprātīgi un datu subjektam pārredzamā veidā;

14.2. nolūka ierobežojuma principu, kas nozīmē, ka personas dati tiek vākti konkrētos, skaidros un leģitīmos nolūkos, un to turpmāku apstrādi neveic ar minētajiem nolūkiem nesavietojamā veidā;

14.3. datu minimizēšanas principu, kas nozīmē, ka personas dati tiek vākti un apstrādāti adekvāti, atbilstīgi un ietver tikai to, kas nepieciešams to apstrādes nolūkos;

14.4. precizitātes principu, kas nozīmē, ka personas dati ir precīzi, ja vajadzīgs, atjaunināti un ir jāveic visi saprātīgi pasākumi, lai nodrošinātu, ka neprecīzi personas dati, ņemot vērā nolūkus, kādos tie tiek apstrādāti, bez kavēšanās tiktu dzēsti vai laboti;

14.5. glabāšanas ierobežojuma principu, kas nozīmē, ka personas dati tiek glabāti veidā, kas pieļauj datu subjektu identifikāciju, ne ilgāk kā nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā; personas datus var glabāt ilgāk, ciktāl personas datus apstrādās tikai arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, vai statistikas nolūkos saskaņā ar Regulas 89. panta 1. punktu, ar noteikumu, ka tiek īstenoti atbilstoši tehniski un organizatoriski pasākumi, kas šajā regulā paredzēti, lai aizsargātu datu subjekta tiesības un brīvības;

14.6. integritātes un konfidencialitātes principu, kas nozīmē, ka personas dati tiek apstrādāti tādā veidā, lai tiktu nodrošināta atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai bojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus;

14.7. pārskatatbildības principu, kas nozīmē, ka pārzinis ir atbildīgs par datu apstrādes atbilstību 14.1. -14.6. norādītajiem principiem un var to uzskatāmi parādīt.

15. Balstoties uz iepriekš norādītajiem principiem, Sistēma tiek veidota tādējādi, lai datu subjektam būtu iespēja:

15.1. piekļūt pārziņa apstrādātajiem datiem un saņemt par tiem informāciju normatīvajos aktos noteiktajā kārtībā un gadījumos (datu subjekta piekļuves tiesība);

15.2. panākt, lai pārzinis bez nepamatotas kavēšanās labotu vai papildinātu neprecīzus datu subjekta personas datus (tiesības labot);

15.3. panākt, lai pārzinis bez nepamatotas kavēšanās dzēstu datu subjekta personas datus, un pārziņa pienākums, normatīvajos aktos noteiktā kārtībā un gadījumos, ir bez nepamatotas kavēšanās dzēst personas datus (tiesības tikt aizmirstam);

15.4. panākt, lai pārzinis ierobežotu apstrādi, ja ir kāds no normatīvajos aktos noteiktajiem apstākļiem (tiesības ierobežot apstrādi);

15.5. saņemt personas datus attiecībā uz sevi, kurus viņš sniedzis pārzinim, strukturētā, plaši izmantotā un mašīnlasāmā formātā un ir tiesības minētos datus nosūtīt citam pārzinim, un pārzinis, kuram attiecīgie personas dati sniegti, normatīvajos aktos noteiktajos gadījumos nerada nekādus šķēršļus (tiesības uz datu pārnesamību).

IV. Sistēmas pārvaldības organizācija un atbildība

16. BAT valde (turpmāk – valde) īsteno Sistēmas ieviešanu un pārvaldību, norīkojot atbildīgās personas un uzraugot atbildīgo personu darbību.

17. BAT struktūrvienības vadītājs atbild par Sistēmas ieviešanu un pārvaldību savā struktūrvienībā, nosaka personālu, kuriem ir piekļuve apstrādājamiem personas datiem, katram nosaka apstrādājamo personas datu veidu, nolūku, atļautos saņēmējus, kā arī kārtību kādā attiecīgās struktūrvienības telpās glabājami personas datus saturoši drukāti dokumenti, savlaicīgi anulē piekļuves tiesības personālam, ar kuru tiek pārtrauktas darba attiecības. Drošības prasības

elektronisko personas datu apstrādei noteiktas atbilstoši BAT informācijas un komunikācijas tehnoloģijas sistēmu drošības politikai;

18. Valde ar rīkojumu nosaka par datu apstrādes un aizsardzības Sistēmu atbildīgo personu (datu aizsardzības speciālistu), kura uzrauga Sistēmas ieviešanu un pārvaldību, kā arī seko normatīvajos aktos noteikto personas datu apstrādes un aizsardzības prasību ievērošanai.

19. Par datu apstrādi un aizsardzības Sistēmu atbildīgā persona sadarbībā ar IT Sistēmu drošības pārvaldnieku pārrauga BAT notiekošos personas datu apstrādes procesus, informē valdi un BAT attiecīgo struktūrvienību vadītājus par atklātajiem riskiem, piedāvā risinājumus risku novēršanai, organizē datu apstrādes pārkāpumu incidentu izmeklēšanu.

20. Par datu apstrādes un aizsardzības Sistēmu atbildīgā persona atbild par BAT datu apstrādes reģistra uzturēšanu aktuālā stāvoklī, organizē personāla apmācību par personas datu apstrādes jautājumiem, sagatavo atbildes uz datu subjektu pieprasījumiem ar datu apstrādi saistītos jautājumos, kā arī normatīvos aktos paredzētos gadījumos informē uzraudzības iestādi – Datu valsts inspekciju.

21. BAT struktūrvienību vadītājiem ir pienākums sadarboties ar personu, kas atbildīga par datu apstrādes un aizsardzības Sistēmu, tai skaitā informējot par pārkāpumiem datu apstrādē, incidentiem, nākotnē paredzamām jaunām datu apstrādes darbībām un jauniem personas datu saņēmējiem, kā arī jebkurām citām notikušām vai paredzamām izmaiņām personas datu apstrādes procesos.

22. Lai novērtētu riskus un uzraudzītu BAT personas datu apstrādes procesu atbilstību iekšējo un ārējo normatīvo aktu noteikumiem ne retāk kā reizi gadā organizējama Sistēmas drošības risku izvērtēšana. Izvērtēšana organizējama sadarbojoties par datu apstrādes un aizsardzības Sistēmu atbildīgai personai, struktūrvienību vadītājiem un IT Sistēmu drošības pārvaldniekam. Ziņojums par risku izvērtēšanas rezultātiem sniedzams valdei un attiecīgo struktūrvienību vadītājiem.

V. Personas datu apstrādes tiesību piešķiršana un anulēšana

23. Personas datu apstrādes tiesību piešķiršanu un anulēšanu, darba tiesisko vai citu līgumisko attiecību nodibināšanas vai pārtraukšanas gadījumā, veic BAT struktūrvienības vadītājs. Savukārt IT Sistēmu drošības pārvaldnieks, atbilstoši BAT informācijas un komunikācijas tehnoloģijas sistēmu drošības politikai, piešķir vai anulē IT Sistēmas lietotāju tiesības.

24. Pirms personas datu apstrādes tiesības piešķiršanas un IT Sistēmas lietotāja tiesības piešķiršanas BAT struktūrvienības vadītājs sadarbībā ar par datu apstrādes un aizsardzības Sistēmu atbildīgo personu iepazīstina BAT personālu ar BAT iekšējiem normatīvajiem aktiem, kuri nosaka personāla tiesības, pienākumus un atbildību saistībā ar personas datu apstrādi un aizsardzību. Personāla tiesības un pienākumi datu apstrādē ir noteikti BAT iekšējos normatīvajos aktos un noslēgtajos līgumos.

25. BAT Struktūrvienības vadītājs vai IT Sistēmu drošības pārvaldnieks, konstatējot personas datu aizsardzības pārkāpumu (incidentu), ir tiesīgi anulēt iesaistītā personāla tiesības apstrādāt personas datus un/ vai anulēt IT Sistēmas lietotāja piekļuves tiesības.

VI. Sistēmas drošības jautājumi

26. Ar IT Sistēmu un elektronisko personas datu nesēju glabāšanu saistītie drošības jautājumi tiek risināti atbilstoši BAT apstiprinātai informācijas un komunikācijas tehnoloģijas sistēmu drošības politikai un uz šīs politikas pamata pieņemtajiem BAT iekšējiem normatīvajiem aktiem;

27. Savukārt papīra (drukātā) formā izgatavoto personas datu nesēju (noslēgto līgumu oriģinālu un kopiju, personas identitāti apliecinošu dokumentu kopijas, personas lietu u.c. dokumentu oriģinālu un kopiju, turpmāk – Dokumenti) glabāšana notiek ievērojot šādus pamatprincipus:

27.1. no Dokumentiem netiek izgatavotas kopijas, kuras nav tieši nepieciešamas atļauto personas datu apstrādes darbību veikšanai;

27.2. dokumenti tiek apstrādāti (glabāti, nodoti, pārsūtīti, u.c.) tādā vietā un veidā, kas pēc iespējas samazina nesankcionētas piekļuves un neatļautu datu apstrādes darbību veikšanas risku;

27.3. dokumenti tiek glabāti ne ilgāk, kā lietu nomenklatūrā noteikts – pēc tam iznīcināti vai nodoti arhīvam.

28. BAT tiek uzturēts personas datu aizsardzības pārkāpumu (incidentu) un datu subjektu pieprasījumu uzskaites reģistrs, ko ved par datu apstrādes un aizsardzības Sistēmu atbildīgā persona. Reģistrā tiek reģistrēti incidenti, kurus atklāj par datu apstrādes un aizsardzības Sistēmu atbildīgā persona, IT Sistēmu drošības pārvaldnieks, BAT struktūrvienību vadītāji vai jebkura cita persona, kura ziņo par notikuši incidentu.

29. Jebkurā gadījumā lēmumu par turpmākām darbībām incidenta izmeklēšanai un seku novēršanai pieņem par datu apstrādes un aizsardzības Sistēmu atbildīgā persona.

30. Par datu apstrādes un aizsardzības Sistēmu atbildīgā persona izstrādā plānu Sistēmas drošas darbības kontrolei, ar Sistēmas darbību saistītie dokumenti tiek aktualizēti pēc nepieciešamības, bet ne retāk kā reizi gadā.

VII. Noslēguma jautājums

31. Kārtību, kādā BAT tiek organizēta Sistēmas ieviešana, pārvaldība un lietošana, nosaka valdes priekšsēdētāja apstiprināti iekšējie normatīvie akti.

Sekretariāta vadītāja L.Mežecka