Rekomendācija

«Personas datu apstrādes drošība»

Rīga

Definīcijas

Cilvēka cieņa ir neaizskarama. Tā ir jārespektē un jāaizsargā.

(Eiropas Savienības Pamattiesību hartas 1.pants)

Ikvienai personai ir tiesības uz savu personas datu aizsardzību.

(Eiropas Savienības Pamattiesību hartas 8.pants)

Personas dati – jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisko personu.

(Fizisko personu datu aizsardzības likums)

Drošība – stāvoklis, apstākļi, kuros nav apdraudējuma un/vai ir vajadzīgā aizsardzība pret iespējamu apdraudējumu.

(LZA Terminoloģijas komisijas apstiprinātā definīcija)

Ievads

Tiesības uz savu privātuma un personas datu aizsardzību kļūst aizvien svarīgākas informācijas tehnoloģiju un interneta attīstības kontekstā. Digitālā revolūcija, izmantojot dažādus informāciju tehnoloģiju resursus, sola ikvienam indivīdam ieguvumus veselības aprūpes, apkārtējās vides un ekonomikas attīstības kontekstā. Turklāt Eiropas Savienības vienotais digitālais tirgus, mākoņdatošana un lietu internets tiek uzskatīti kā būtiskākie elementi Eiropas Savienības valstu ekonomiskajai izaugsmei un attiecīgi iedzīvotāju labklājības veicināšanai. Ņemot vērā minēto, svarīga ir pārziņu atbildība par veikto personas datu apstrādi, izvēloties tādus personas datu apstrādes risinājumus, kas ir droši no personas datu apstrādes un aizsardzības viedokļa un respektē indivīda privātumu.

Fizisko personu datu aizsardzības likums definē, ka personas dati ir jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisko personu. Savukārt, uz šī likuma pamata izstrādātie Ministru kabineta 2001. gada 30. janvāra noteikumi Nr. 40 „Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības" nosaka, ka personas dati ir aizsargājami gan ar fiziskiem aizsardzības līdzekļiem pret fiziskās iedarbības radītu apdraudējumu, gan arī ar loģiskās aizsardzības līdzekļiem – ar programmatūras līdzekļiem, parolēm, šifrēšanu, kriptēšanu un citiem. Šajā normatīvajā aktā arī teikts, ka tikai atbilstošām

darbībām pilnvarotas personas drīkst personas datus apstrādāt – vākt, reģistrēt, ievadīt, glabāt, sakārtot, pārveidot, izmantot, nodot, pārraidīt un izpaust, bloķēt vai dzēst.

Saskaņā jau ar spēkā esošajiem normatīvajiem aktiem, veicot fizisko personu datu apstrādi, ikvienam pārzinim ir jānodrošina šādu labas prakses principu ievērošana:

- *dati tiek godīgi un likumīgi apstrādāti;*
- *datu apstrāde tiek veikta konkrētiem mērķiem un tikai saskaņā ar tiem;*
- *dati ir adekvāti (ne pārmērīgi);*
- *dati ir precīzi;*
- *dati netiek glabāti ilgāk kā nepieciešams konkrēta mērķa sasniegšanai;*
- *dati tiek apstrādāti saskaņā ar datu subjekta tiesībām;*
- *dati ir drošībā;*
- *dati netiek pārsūtīti uz citām organizācijām, iestādēm vai ārvalstīm bez drošas un adekvātas aizsardzības.*

Aizvien biežāk personas datu apstrāde tiek veikta īstenojot visdažādākos ikdienas pienākumus. Drošu un likumdošanai atbilstošu IT sistēmu uzturēšana var būt komplicēts uzdevums, kura veikšanai nepieciešams gan laiks, gan līdzekļi, gan arī speciālas zināšanas. Ja jūsu IT sistēmās tiek apstrādāti personas dati, tas rada papildu riskus. Lai panāktu, ka datu apstrāde ir droša un uzticama, paaugstinātais riska līmenis ir jāapzinās un jāveic normatīvo aktu prasībām, kā arī jūsu organizācijas iespējām un vajadzībām atbilstoši, tehniski pasākumi. Tiem ne vienmēr jābūt dārgiem vai pārlieku sarežģītiem. Daudzus no šajā rekomendācijā minētajiem pasākumiem var ieviest ar nelieliem finanšu ieguldījumiem un daudzi, iespējams, jau pašlaik ir jūsu rīcībā. Svarīgi personas datu apstrādes un aizsardzības jautājumus izvērtēt pirms personas datu apstrādes uzsākšanas, kas savlaicīgi ļaus izvēlēties piemērotākos IT resursus personas datu apstrādei.

Šī rekomendācija paredzēta nelielām organizācijām un uzņēmumiem kā praktisku padomu kopums IT drošības jautājumos no personas datu aizsardzības viedokļa.

Kāpēc jums tas vajadzīgs?

Nodrošināta adekvāta personas datu apstrāde un aizsardzība sekmē uzticēšanos Jūsu sniegtajiem pakalpojumiem, jo ikviens indivīds novērtē to, ka viņa/ viņas personas dati ir drošībā.

Turklāt par personas datu apstrādes noteikumu pārkāpumiem juridiskai personai var piemērot administratīvo sodu līdz pat 14 000 EUR. Gadījumos, kad pārkāpumi konstatēti nolaidības vai ļaunprātības rezultātā, kā arī, ja radīts būtisks kaitējums, iespējama pat kriminālatbildība. Jāņem vērā, ka personas datu apstrādes pārkāpumu rezultātā var neglābjami ciest uzņēmuma vai iestādes reputācija, kā arī klientu, sadarbības partneru un darbinieku uzticība. Lai arī pilnībā nodrošināties pret negadījumiem nav iespējams, laicīgi ieviešot noteiktu pasākumu kopumu, līdz minimumam var ierobežot ļaunprātīgas rīcības radīto ietekmi un sekas.

Pirmkārt, izvērtējiet risku, ko personas datu apstrādes drošības incidenti var radīt jūsu organizācijai. Pirms izlemt, kāda līmeņa aizsardzība jūsu gadījumā būtu vispiemērotākā, ir jānovērtē, kādi personas dati ir jūsu rīcībā un kādiem riskiem tie ir pakļauti. Šajā procesā jāņem vērā visi datu apstrādes posmi – gan iegūšana un uzglabāšana, gan izmantošana un iznīcināšana (tajā skaitā, ārpakalpojumu izmantošana kādā no personas

datu apstrādes procesiem un ar to saistītie iespējamie riski). Novērtējiet, cik vērtīga un konfidenciāla ir informācija, kas ir jūsu rīcībā, un kādu ietekmi uz konkrētajām personām varētu atstāt tās noplūde drošības incidenta gadījumā. Kad ir apzināts iespējamo risku kopums, varat sākt izvērtēt jūsu situācijai atbilstošu drošības pasākumu ieviešanu.

Valsts un pašvaldību institūcijām, kurām deleģēti pārvaldes uzdevumi, saskaņā ar Fizisko personu datu aizsardzības likuma 26. panta otro daļu, jāsagatavo personas datu apstrādes atbilstības novērtējums, ietverot tajā arī riska analīzi un pārskatu par informācijas drošības jomā veiktajiem pasākumiem. Nosacījumus personas datu apstrādes atbilstības novērtējumam, tā sagatavošanas un iesniegšanas kārtību, kā arī termiņu nosaka Ministru kabinets.

Drošības paaugstināšanas pasākumos ieteicams izmantot vairāklīmeņu pieeju, jo viena simtprocentīgi droša risinājuma nav. Efektīva rezultāta sasniegšanai nepieciešama sistēma, kas sastāv no vairākām komponentēm un apvieno dažādus līdzekļus un tehnoloģijas – ja uzbrucējam izdodas apiet vienu, viņu, iespējams, var apturēt pārējās.

Vairāklīmeņu drošība[1]

Fiziskā aizsardzība

Iekļūstot jūsu telpās, būs iespējams fiziski piekļūt iekārtām un IT resursiem, kuros glabājas personas dati. Jums jānodrošina, ka personas dati šajās iekārtās ir aizsargāti. Serveri jāizvieto atsevišķās telpās ar pastiprinātu aizsardzību. Rezerves kopiju iekārtas nedrīkst atstāt brīvi pieejamas un bez attiecīgas kontroles, tās pēc lietošanas jāieslēdz seifā vai jāpārvieto citā drošā vietā. Tomēr adekvāti fiziskās drošības principi un to regulāra kontrole jānodrošina arī telpās, kur notiek personas datu apstrāde vai kurās atrodas jūsu IT sistēmas.

Aizsardzība pret datorvīrusiem un ļaunatūru[2]

Lai konstatētu un novērstu ievainojamības datu tīklā un lietotāju datoros, jānodrošina pastāvīga kontrole aizsardzībai pret datorvīrusiem, ļaunatūru un citiem līdzīgiem draudiem. Lai tā būtu efektīva, jāraugās, lai drošības programmatūra tiktu regulāri atjaunināta. Ja jums ir nepieciešams, piesaistiet konsultantu šajos jautājumos, jo atcerieties, ka kopumā par veikto personas datu apstrāde un tās aizsardzību atbild pārzinis. Tādēļ pārliecinieties, ka Jūs nodrošināt atbilstošu drošību.

Aizsardzība pret ārēju ielaušanos

Jūsu IT sistēmai jābūt spējīgai novērst ārēju nesankcionētu piekļuvi datiem, neļaujot uzbrucējam iekļūt jūsu datu tīklā. Piemēram, to var nodrošināt ar pareizi konfigurēta ugunsmūra palīdzību.

Piekļuves kontrole

Piekļuves tiesību sadalījums ir viens no jautājumiem, kuram pārziņi nereti nepievērš pienācīgu uzmanību.

1 Izmantoti ieteikumi no Liebritānijas Informācijas komisāra biroja (ICO) vadlīnijām.

2 Ļaunatūra – ļaunprātīga programmatūra (angļu val. – malware).

Nodrošiniet piekļuvi informācijas sistēmām, kurās ir personas dati, tikai noteiktiem pilnvarotiem lietotājiem vai tikai jūsu pārvaldībā esošām iekārtām. Katram lietotājam jāpiešķir savi atšķirīgi autentifikācijas līdzekļi – lietotāja vārds un parole, kura regulāri drošības nolūkā jāmaina.

Paroļu uzlaušana ar „rupja spēka"[3] metodi ir ļoti izplatīts uzbrukuma veids, ko, jums nezinot, var izmantot pat jūsu kaimiņš, piemēram, mēģinot uzminēt jūsu bezvadu tīkla paroli. Sistēmās jānosaka minimālais paroļu komplicētības līmenis, jāierobežo maksimālais neveiksmīgu autorizācijas gadījumu skaits un jāveic regulāra paroļu maiņa.

Lietotāja konti un citi autentifikācijas līdzekļi jābloķē nekavējoties pēc darba tiesisko attiecību izbeigšanas ar konkrētu darbinieku, kā arī darbiniekam esot ilgstošā prombūtnē.

Darbinieku informētības paaugstināšana un apmācība

Visiem organizācijas darbiniekiem jābūt informētiem par savu lomu un atbildību organizācijas drošības politikā. Apmāciet darbiniekus atpazīt tādus draudus kā „pikšķerēšanas"[4] e-pasta ziņojumi vai citu ļaunatūru, un informējiet, kā rīkoties gadījumos, kad, iespējams, ir notikusi nelikumīga datu apstrāde, lai pēc iespējas ātrāk būtu iespējams šādu pārkāpumu novērst.

Svarīgi, lai darbinieki zinātu, kādu rīcību no viņiem sagaidāt gadījumā, ja tiek konstatēts drošības pārkāpums, kā arī viņiem jābūt informētiem par gadījumiem, kad kāds ļaunprātīgi, apmānot darbiniekus, varētu mēģināt izkrāpt personas datus. Darbiniekus svarīgi informēt arī par sekām, kas iestāsies gadījumā, ja darbinieks apzināti un bez attiecīga pilnvarojuma izpaudīs citu personu personas datus.

Segmentācija

Novērst incidentus vai samazināt to ietekmi var, nodalot tīkla iekārtas un ierobežojot komunikāciju starp tām. Piemēram, serveri, kas nodrošina organizācijas tīmekļa vietnes darbību, var izvietot atsevišķā apakštīklā no datu servera. Tas nozīmē, ka sekmīgi realizēts uzbrukums jūsu interneta vietnei negarantē uzbrucējam pieeju citiem datiem.

Politika un risku pārvaldība

IT politikas dokumentācijas izstrāde liecina, ka jūsu organizācija pienācīgi rūpējas par risku samazināšanu vai

3 Autorizācijas mēģinājumi, pielietojot visbiežāk lietotās zināmās paroles vai ar sistemātisku iterāciju palīdzību ģenerējot burtu, ciparu un simbolu kombinācijas (angļu val. – brute force).

4 Pikšķerēšana – nelikumīgs veids, kā ar viltu iegūt interneta lietotāja informāciju, piemēram, lietotāju vārdus, paroles, kredītkaršu numurus utt. (angļu val. – phishing).

novēršanu. Efektīvas un jūsu organizācijai atbilstošas instrukcijas, plāni un politikas dokumenti būs vērtīgs papildinājums risku izvērtēšanā un organizācijas pārvaldības procesu uzlabošanā kopumā. IT politikas dokumentācijai ir jābūt atbilstošai Jūsu darbības specifikai un reāli īstenojamai.

Iekārtu drošības uzlabošana

Atinstalējiet programmatūru, kas netiek lietota, un atslēdziet nevajadzīgos pakalpojumus darbstacijās un serveros. Gandrīz visām visbiežāk lietoto programmu iepriekšējām versijām ir konstatētas un plaši zināmas drošības ievainojamības. Ja programmas netiek lietotas, vieglāk ir tās atinstalēt nekā nodrošināt, lai būtu uzstādīti visi drošības ielāpi un jauninājumi.

Īpaši pārliecinieties, ka jūsu programmatūra un iekārtas neizmanto sākotnējās konfigurācijas paroles (admin-admin u.tml.) – tās arī potenciālajiem uzbrucējiem ir ļoti labi zināmas.

Gadījumos, kad nolietotās IT iekārtas vēlaties nodot utilizēšanai, pārliecinieties, ka tiek dzēsti visi personas dati (piemēram, pirms nododat utilizēt savu veco datoru, izņemiet cieto disku un to atbilstoši iznīciniet).

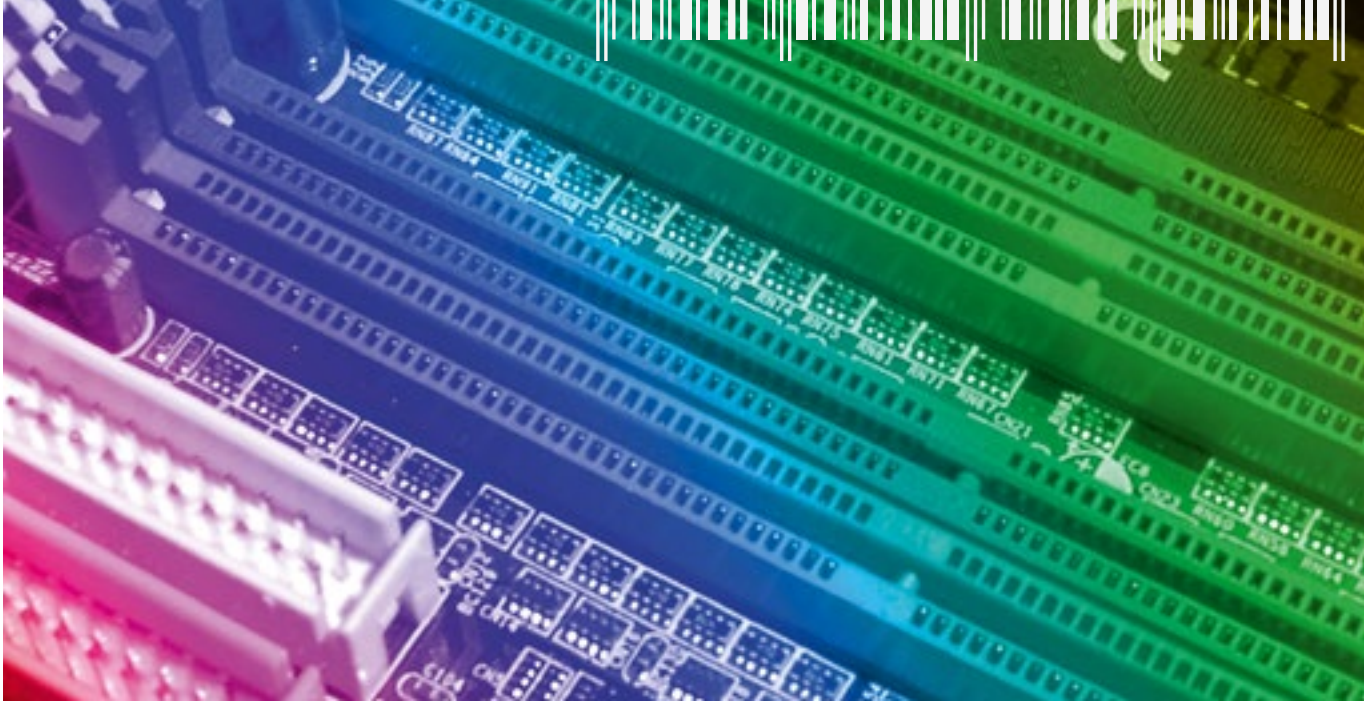
Datu drošība ārpus biroja

Mūsdienās aizvien biežāk tiek izmantota prakse strādāt ārpus biroja telpām, pateicoties informāciju piedāvātajām tehnoloģiju iespējām. Tāds pats drošības līmenis kā birojā ir jānodrošina arī ierīcēs, kas tiek lietotas ārpus biroja – portatīvajos datoros, mobilajos tālruņos un viedtālruņos, ārējos cietajos diskos un zibatmiņas ierīcēs. Neskaitāmi datu noplūdes un drošības incidenti notiek gadījumos, kad iekārtas tiek pazaudētas vai nozagtas. Lai samazinātu risku iekārtas zaudējuma gadījumā, vajadzētu nodrošināt, ka personas datu šajās iekārtās nav vispār, vai arī šai informācijai nav iespējams piekļūt bez atbilstošas autorizācijas. Paaugstināts drošības risks ir arī datiem, kas tiek sūtīti pa e-pastu, pastu vai izmantojot kurjerdienestu.

Datu šifrēšana ir viens no izplatītākajiem paņēmieniem, kā mobilajās ierīcēs nodrošināt piekļuvi datiem tikai pilnvarotām personām. Datu „atslēgšanai" parasti nepieciešama parole. Šifrēšanas parolei jābūt veidotai gan no lielajiem un mazajiem burtiem, gan cipariem, gan speciālajiem simboliem (piemēram, !@%). Šifrēt iespējams gan visu datora cieto disku, gan atsevišķas datnes.

Atsevišķas datorprogrammas nodrošina iespēju aizsargāt datnes pret izmaiņu veikšanu, tomēr šāda aizsardzība neatturēs ļaundari no datu iegūšanas. Turklāt, šādu aizsardzību vairumā gadījumu diezgan vienkārši iespējams apiet, izmantojot brīvi pieejamus publiskus tīmekļa resursus. Iesakām pārliecināties, ka katrā konkrētajā gadījumā pielietojat pareizo aizsardzības metodi.

Atsevišķas mobilās iekārtas nodrošina iespēju veikt attālinātu datu dzēšanu vai ierīces bloķēšanu, nosūtot atbilstošu signālu pazudušajai vai nozagtajai iekārtai.



Tomēr šādam – visbiežāk maksas – pakalpojumam ierīces parasti jāreģistrē un jāpieslēdz, pirms noticis incidents.

Personas datus uz mobilajām ierīcēm pārnesiet tikai tad, ja tas ir patiešām nepieciešams, un izdzēsiet tos, kad šāda nepieciešamība beidzas.

Nodrošiniet regulārus atjauninājumus

Datortehnikai un programmatūrai nepieciešama pastāvīga apkope, lai tās strādātu efektīvi un ar ierobežotu drošības ievainojamības risku. Drošības programmatūrai, piemēram, pretvīrusu risinājumiem, svarīgi regulāri uzstādīt atjauninājumus, lai nodrošinātu adekvātu aizsardzību.

Pārliecinieties, ka drošības programmatūra, kuru lietojat, ir aktīva un pastāvīgi skenē svarīgākās datnes, direktorijas un diskus.

Regulāri uzstādiet programmatūras atjauninājumus un operētājsistēmas drošības ielāpus. Lielākajai daļai sistēmu iespējams uzstādīt automātisku šā procesa norisi.

Ne retāk kā reizi gadā pārbaudiet, vai jūsu lietotie drošības risinājumi atbilst aktuālajai situācijai un prasībām.

Pastāvīgi uzlabojiet kompetences līmeni fizisko personu datu aizsardzības un drošības jautājumos, it īpaši tajos, kas raksturīgi jūsu darbības nozarei. Piemēram, sekojiet līdzi drošības ziņām tīmeklī vai izmantojiet iespējas saņemt attiecīga satura ziņojumus e-pastā.
Informējiet darbiniekus un kolēģus par iespējamiem drošības draudiem personas datu apstrādes kontekstā un riskiem jūsu organizācijā. Izglītojiet darbiniekus un

informējiet par riskiem, kas rodas, pārsūtot organizācijas iekšējo informāciju, izmantojot sociālos tīklus vai mākoņdatošanas pakalpojumus. Iemāciet darbiniekiem atpazīt pikšķerēšanas e-pasta ziņojumus.

Datu apstrāde „mākonī"

Arvien biežāk uzņēmumi un organizācijas datu pieejamības uzlabošanai datu apstrādi un uzglabāšanu izvēlas veikt, izmantojot tā saucamo mākoņdatošanu[5]. Lai gan šāda datu apstrāde tiek uzskatīta par progresīvu, jūsu pienākums un atbildība ir sekot, lai dati būtu drošībā, kaut arī tie fiziski neatrodas jūsu iekārtās vai jūsu telpās.

Pievērsiet uzmanību mākoņdatošanas pakalpojumiem gan tad, kad tos izmantojat paši, gan tad, kad tos izmanto ārpakalpojuma sniedzējs, lai sniegtu konkrētu pakalpojumu jums. Mākoņdatošanas pakalpojumu ietvaros organizācijām tiek piedāvātas aizvien jaunas iespējas arī attiecībā uz personas datu apstrādi (īpaši uz datu saglabāšanu), tomēr ne vienmēr tiek identificēti riski šādu pakalpojumu izmantošanā. Pirms jūs izvēlaties izmantot mākoņdatošanas pakalpojumus, izvērtējiet, piemēram, kas varēs piekļūt jūsu saglabātajiem datiem „mākonī" – tikai jūs (izvērtējiet nosacījumus, kas attiecas uz pakalpojuma sniedzēja piekļuves tiesībām jūsu saglabātajiem personas datiem „mākonī"), vai informācija būs publiski pieejama, vai būs dalīta piekļuve (tikai pilnvarotām personām). Atcerieties, ka jūsu kā pārziņa pienākums ir nodrošināt adekvātus personas datu aizsardzības risinājumus visā personas datu apstrādes procesā.

5 Datu glabāšanas, skaitļošanas jaudas vai programmatūras pakalpojumu pirkšana no citas kompānijas, piekļūstot šiem resursiem caur internetu.

Ieteikums pirms līgumisko attiecību noslēgšanas ar ārpakalpojumu sniedzēju par mākoņdatošanas pakalpojumiem – palūdziet mākoņpakalpojuma sniedzējam atzītas auditorkompānijas drošības audita atzinumu vai atzītu pakalpojuma kvalitātes sertifikātu. Izvērtējiet, vai šie dokumenti nodrošina, ka iespējamais datu apstrādes un aizsardzības riska līmenis būs jums pieņemams.

Pakalpojuma sniedzējam jāreaģē nekavējoties, ja viņa sniegtajā pakalpojumā vai izmantotajā programmatūrā tiek konstatēta ievainojamība.

Elektroniskā komunikācija starp pakalpojuma sniedzēju un jums kā pakalpojuma saņēmēju jāšifrē, piemēram, izmantojot uzticamu trešās puses izsniegtu elektronisko sertifikātu. Ieteicams pakalpojumu sniedzēja uzglabātos datus šifrēt uzglabāšanas vietā, nosakot precīzu kārtību, – kas un kādā veidā atbild par attiecīgo šifru atslēgām, parolēm un sertifikātiem.

Veicot personas datu apstrādi „mākonī", pakalpojumu sniedzējs kļūst par personas datu operatoru, ar kuru jums kā pārzinim jānoslēdz rakstveida līgums (Fizisko personu datu aizsardzība likuma 14. panta pirmā, otrā daļa). Neaizmirstiet arī noskaidrot, kā pakalpojumu sniedzējs informēs jūs par iespējamām izmaiņām pakalpojuma sniegšanā.

Pakalpojumu sniedzējam jānodrošina jums iespēja kontrolēt kurš, kad un kādiem datiem piekļūst. Parasti to nodrošina sistēmu auditācijas pieraksti.

Pirms izvēlēties mākoņpakalpojuma sniedzēju, izvērtējiet, vai tam būs pietiekami resursi un rezerves jaudas, lai nodrošinātu, ka jūsu saņemto pakalpojumu neietekmēs pakalpojuma sniedzēja citu klientu noslodze, un

tādējādi jūs vienmēr varēsit saņemt pakalpojumu tad, kad tas būs nepieciešams.

Novērtējiet pakalpojuma pieejamības līmeni. Cik ātri pakalpojumu sniedzējs apņemas atjaunot datus no rezerves kopijas, ja notiek nopietns datu zudums? Vai pakalpojumu sniedzējs var jebkurā brīdī jūs nodrošināt ar pilnu datu kopiju jums pieņemamā formātā?

Fizisko personu datu aizsardzības likums (t.sk. likuma 28. pants) stingri reglamentē datu nodošanu uz citām valstīm. Uzdodiet pakalpojumu sniedzējam jautājumu – kurās valstīs būs pieejami (tajā skaitā – glabāti) jūsu organizācijas pārziņā esošie personas dati un, vai ir iespējams iegūt informāciju par personas datu aizsardzības līmeni šajās valstīs? Pavaicājiet par nosacījumiem, kādos jūsu dati var tikt nodoti uz citām valstīm, piemēram, izvietošanai citā pakalpojumu sniedzēja datu centrā. Vai pakalpojumu sniedzējs var nodrošināt jums valstu izvēles iespējas, ja šāda datu nodošana notiktu?

Gadījumā, ja lauzīsiet līgumu ar pakalpojumu sniedzēju par mākoņdatošanas pakalpojumu sniegšanu, viņam jūsu dati un visas rezerves kopijas ir jāiznīcina.

Ieviesiet kontroles pasākumus

Kibernoziedznieki un ļaunatūra pastāvīgi apdraud jūsu IT sistēmas, tomēr lielā daļā sistēmu uzbrukuma fakti tiek konstatēti novēloti, lai gan pazīmes dažkārt tiek novērotas jau ilgstoši.

Regulāri pārbaudiet drošības programmatūras ziņojumus, sistēmu un aplikāciju žurnālfailus un citas atskaišu sistēmas, kas ir jūsu rīcībā.

Izveidojiet metodi, kā pastāvīgi kontrolēt, kādas programmas un pakalpojumi ir aktīvi jūsu datu tīklā, identificējot un bloķējot aizdomīgās darbības.

Regulāri veiciet ievainojamības pārbaudes un ielaušanās testus, lai pārbaudītu sistēmu izturību. Nekavējieties ar pretpasākumu ieviešanu, ja konstatējat nepilnības.

Nosakiet prioritātes

Daudzās organizācijās IT sistēmu aizsardzības līmenis ir nepietiekams tikai tādēļ, ka nav korekti pielietotas esošās drošības procedūras un pašas organizācijas nespēj konstatēt, kur un kāpēc var rasties problēmas. Tādēļ ir ne tikai jāizstrādā reāls plāns rīcībai incidentu gadījumos, bet arī jāinformē visi darbinieki par viņu lomu un atbildību ikdienas situācijās.

Sastādiet pārskatu, kādi personas dati ir jūsu organizācijas rīcībā un kādi aizsardzības līdzekļi tiem ir piemēroti. Apziniet riskus visiem jūsu pārziņā esošo personas datu veidiem. Izplānojiet rīcību gadījumos, ja notiktu šo datu noplūde.

Nosakiet savas organizācijas darbības atbilstību normatīvajiem aktiem, vadlīnijām un labās prakses piemēriem, kas raksturīgi jūsu pārstāvētajai nozarei. Izstrādājiet sistēmu lietošanas politikas dokumentus un apmācību materiālus darbiniekiem, lai viņi apzinātos savu atbildību personas datu aizsardzībā. Atcerieties, ka saskaņā ar Ministru kabineta 2001. gada 30. janvāra noteikumu Nr. 40 „Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības" 5. punktu katram pārzinim ir pienākums izstrādāt iekšējos datu apstrādes aizsardzības noteikumus, tajos nosakot vismaz šajā punktā minētos datu aizsardzības aspektus. Savukārt, saskaņā ar Fizisko personu datu aizsardzības likuma 27. panta pirmo daļu pārzinim jānodrošina, ka fiziskās personas, kuras tiek iesaistītas personas datu apstrādē, rakstveidā apņemas saglabāt un nelikumīgi neizpaust personas datus, un šo personu pienākums ir neizpaust personas datus arī pēc darba tiesisko vai citu līgumā noteikto attiecību izbeigšanās.

Aprakstiet iekšējās kontroles procedūras un nosakiet, kurās struktūrās nepieciešami drošības uzlabojumi. Pieaiciniet drošības ekspertu IT sistēmu pārbaudei, lai palīdzētu noteikt, kuri uzlabojumi ir visnepieciešamākie. Kad uzlabojumi ieviesti, turpiniet uzraudzīt kontroles procedūras un veiciet korekcijas, kur nepieciešams.

Neaizmirstiet par datu rezerves kopijām. Tās jāveido regulāri, jātur drošībā un drošā veidā jāiznīcina, kad vairs nav vajadzīgas.

Samaziniet datu apjomu

Fizisko personu datu aizsardzības likums nosaka, ka pārzinim jānodrošina personas datu apstrāde tikai atbilstoši paredzētajam mērķim un tam nepieciešamajā apjomā, kā arī ne ilgāk par katram apstrādes mērķim noteikto laikposmu. Ja laika gaitā jums ir uzkrājies liels personas datu apjoms, iespējams, ka daļa no tiem vairs nav precīzi, zaudējuši nozīmi vai vienkārši kļuvuši lieki. Aktualizējiet jautājumu, vai jums nepieciešams veikt personas datu apstrādi, jo, iespējams, datu apstrādes mērķis ir sasniegts un datus var dzēst. Regulāri pievērsiet uzmanību personas datu aizsardzībai, tostarp skaidrojot darbiniekiem, kas tiek saprasts ar jēdzieniem „personas dati" un „personas datu apstrāde".[6]

Izlemiet, vai jums šie dati joprojām ir vajadzīgi un vai tie glabājas pareizajā vietā. Ja jūsu pārziņā ir vēsturiski dati, kas uzglabājami arhivācijas nolūkiem, un nav nepieciešams tiem piekļūt regulāri, pārvietojiet tos uz drošāku vietu, piemēram, iekārtu, kas nav pieejama tiešsaistē vai tīklā. Tādējādi iespējams samazināt nesankcionētas piekļuves iespējamību.

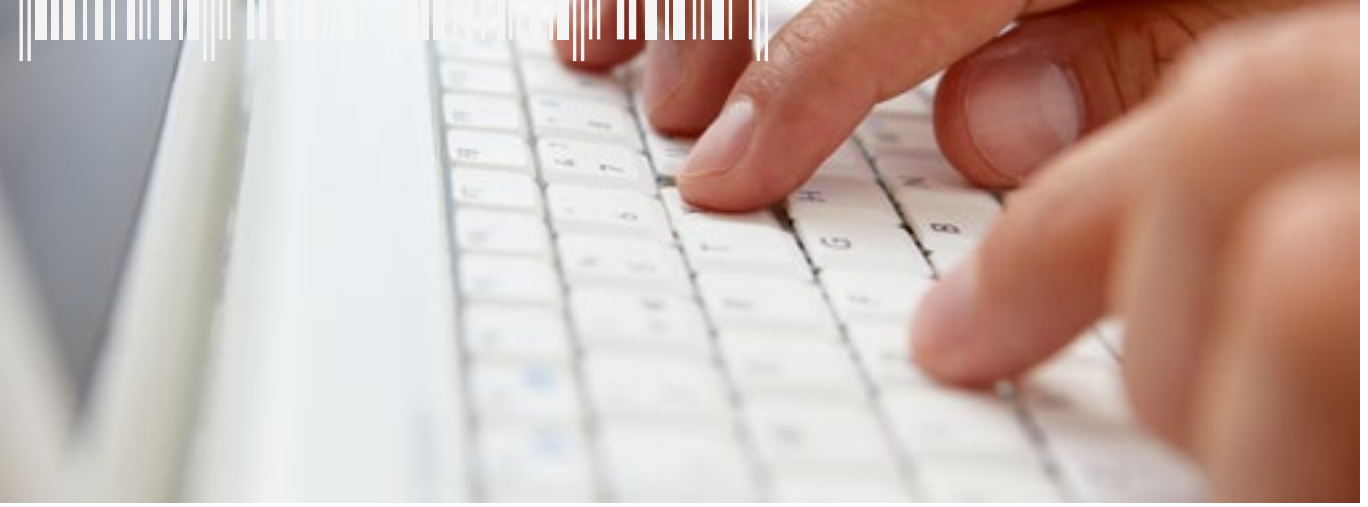
Ja jūsu rīcībā ir dati, kas vairs nav vajadzīgi, tie jāiznīcina. Lai datu iznīcināšanu veiktu atbilstoši drošības prasībām, iespējams, būs nepieciešama speciāla datorprogrammatūra vai ārpakalpojums. Drošības prasības jāievēro, arī iznīcinot papīra formātā saglabātos personas datus.

6 Datu valsts inspekcijas izstrādātā rekomendācija „Personas datu definīcija": http://www.dvi.gov.lv/lv/jaunumi/publikacijas/

Kontrolējiet pakalpojumu sniedzējus

Daudzi nelieli uzņēmumi un organizācijas savu IT sistēmu apkalpošanu uztic trešajām personām – pakalpojumu sniedzējiem. Tomēr, pirms piesaistīt IT atbalsta personālu no ārienes, būtu jāpārliecinās par tā reputāciju, kompetences līmeni, spēju ievērot datu aizsardzības principus un konfidencialitātes prasības.

Veiciet neatkarīgu savu personas datu apstrādes sistēmu drošības auditu vai personas datu apstrādes iekšējo auditu, kura rezultātus izvērtējiet un turpmākās



veicamās darbības izplānojiet kopā ar IT pakalpojumu sniedzēju.

Regulāri caurskatiet IT personāla/pakalpojumu sniedzēja sagatavotās drošības stāvokļa novērtējuma atskaites.

Ja uzskatāt par vajadzīgu, apmeklējiet pakalpojumu sniedzēja telpas, lai pārliecinātos, ka tās atbilst jūsu priekšstatam par apstākļiem, kādos jānotiek drošai pakalpojuma sniegšanai.

Pārbaudiet noslēgtos līgumus ar pakalpojumu sniedzējiem. Tiem jābūt rakstiskiem un tajos jāiekļauj prasības pakalpojumu sniedzējam rīkoties tikai saskaņā ar jūsu prasībām, kā arī ar Fizisko personu datu aizsardzības likuma un citu likumu normām. Slēdzot līgumu, izvērtējiet, vai tam jāatbilst Fizisko personu datu aizsardzības likuma 14. panta prasībām.

Neesiet vieglprātīgi pret iekārtu iznīcināšanu – ja izmantojat ārpakalpojumu datu dzēšanai vai iekārtu drošai iznīcināšanai, pārliecinieties, ka tas tiek veikts adekvāti. Jūs joprojām esat atbildīgs par informāciju, ko satur jūsu iekārtas, – pat tad, ja tās nonāk otrreizējā tirgū.

Pārbaudes jautājumu saraksts, izvērtējot datu drošību Jūsu uzņēmumā

Ja Jūs veicat savu darbinieku, klientu, piegādātāju personas datu apstrādi, tas ir Jūsu pienākums aizsargāt šo informāciju, nodrošinot tās drošu apstrādi (tai skaitā saglabāšanu). Pamatprincipi, kurus Jums nepieciešams nodrošināt:

- *Ievāciet un saglabājiet tikai to informāciju, kas Jums nepieciešama konkrētajam mērķim.*
- *Nodrošiniet, ka personas dati pie Jums ir drošībā.*
- *Pārliecinieties, ka personas dati, kas ir Jūsu rīcībā, Jums joprojām ir nepieciešama, un tā ir aktuāla.*
- *Atbildiet uz datu subjekta informācijas pieprasījumiem, saistībā ar konkrētā indivīda personas datiem, kas ir Jūsu rīcībā.*

Par veikto personas datu apstrādi, pārdomājiet un atbildiet uz šādiem jautājumiem:

- *Vai personas, kuru personas dati ir Jūsu rīcībā, par to ir informēti, kā arī zina, kur un kāpēc Jūs šos personas datus izmantosim?*
- *Vai Jūs esat pārliecināti par to, ka personas dati uzņēmumā tiek droši aizsargāti (gan papīra formātā, gan elektroniski)?*
- *Vai Jūs esat pārbaudījuši savas interneta mājas lapas drošību?*
- *Vai informācija par uzņēmuma darbiniekiem ir aktuāla un precīza?*
- *Vai uzņēmumā personas dati tiek dzēsti nekavējoties, kad sasniegts to apstrādes mērķis un līdz ar to personas dati uzņēmumam vairs nav nepieciešami?*
- *Vai piekļuve personas datiem uzņēmumā ir paredzēta tikai tiem darbiniekiem, kuriem piekļuve šai informācijai ir tiešām nepieciešama darba pienākumu veikšanai?*
- *Pirms uzņēmuma darbinieku personas datu publiskošanas (piemēram, vārds, uzvārds, fotoattēls), vai ir prasīts darbinieku viedoklis par to un saņemta darbinieku piekrišana?*
- *Ja uzņēmums izmanto videonovērošanu, vai tā tiek veikta saskaņā ar normatīvo aktu prasībām personas datu aizsardzības jomā? Ja tas ir tā, vai ir izvietotas atbilstošas informatīvās zīmes par veikto videonovērošanu?*
- *Vai videonovērošanas kameras ir izvietotas tā, lai pēc iespējas mazāk iejauktos indivīdu privātumā?*
- *Vai uzņēmuma darbinieki, kas ikdienā veic personas datu apstrādi, ir atbilstoši apmācīti darbam ar tiem un darbinieki nodrošina personas datu aizsardzību praksē?*
- *Ja uzņēmumā tiek saņemts informācijas pieprasījums par kādu fizisku personu, vai un kurš uzņēmumā zina, vai un kā uz šādu informācijas pieprasījumu atbildēt?*
- *Vai uzņēmums zinātu kā rīkoties, ja uzņēmuma darbinieks, klients vai piegādātājs pieprasītu informāciju par sevi, kas ir uzņēmuma informācijas sistēmās?*
- *Vai uzņēmumā ir noteikta kārtība (piemēram, rīkojums) par personas datu apstrādes veikšanu un aizsardzību?*
- *Vai uzņēmums ir informēts, kādos gadījumos var vērsties Datu valsts inspekcijā un saņemt informāciju par dažādiem personas datu aizsardzības jautājumiem?*
- *Ja uzņēmums ir vienreiz iesniedzis personas datu apstrādes reģistrācijas iesniegumu un personas datu apstrāde ir reģistrēta, vai šim jautājumam kādreiz atkal tiek pievērsta uzmanība un tiek aktualizēta sniegtā informācija?*

Attiecībā uz personas datu apstrādi, kuru uzņēmums veic interneta vidē, iesakām praksē izmantot turpmāk minētos labās prakses principus personas datu apstrādei:

- *Neprasiet indivīdiem autorizēties vai reģistrēties uzņēmuma mājas lapā, vai sniegt identificējošu informāciju par sevi, ja uzņēmumam tā nav nepieciešama pakalpojumu sniegšanai indivīdam. Ir pieņemams, ja pieprasāt kontaktinformāciju no potenciālajiem klientiem, lai ar viņiem sazinātos, bet arī tad – domājiet par nepieciešamās informācijas apjomu.*

- *Pirms Jūs pieprasāt personas datus, sniedziet informāciju par savu uzņēmumu, un norādiet,*

kādēļ tieši uzņēmumam nepieciešams saņemt konkrētu informāciju no klientiem.

- *Uzņēmumam, veicot personas datu apstrādi (tai skaitā datu glabāšanu), ir nepieciešams nodrošināt datu drošību. Ja izmantojat ārpakalpojumus savu informācijas resursu vai sistēmu uzturēšanai, jautājiet šī ārpakalpojuma sniedzējam par iespējām personas datus šifrēt un nodrošiniet, ka uzņēmuma darbinieki par šādiem personas datu apstrādes drošības jautājumiem tiktu apmācīti. Pārliecinieties, ka uzņēmumam ir noslēgts rakstveida līgums ar pakalpojuma sniedzēju, kurā ir noteikta pakalpojuma sniedzēja atbildība, tai skaitā lai nodrošinātu personas datu apstrādes drošību.*

- *Iespējams, ka Jūsu uzņēmuma interneta mājas lapa satur trešo personu informāciju (piemēram, cita uzņēmuma pakalpojumu reklāmu). Attiecīgi Jums ir jābūt gataviem sniegt informāciju, vai un kādu informāciju par Jūsu klientiem saņem tie uzņēmumi, kas ir izvietojuši savu komerciālo informāciju (reklāmu) Jūsu uzņēmuma Interneta mājas lapā.*

Kur iegūt vairāk informācijas?

Kā redzams no šajā rekomendācijā aprakstītajām tēmām, IT sistēmu drošība var būt sarežģīts uzdevums, kam nepieciešams gan laiks, gan finanšu līdzekļi, gan regulārs speciālista padoms. Bet šie pasākumi ir ļoti būtiski, lai jūs veiktu personas datu apstrādi atbilstoši normatīvo aktu prasībām.

Šajā rekomendācijā nav precīzu ieteikumu un gatavu atbilžu, jo katra organizācija personas datu apstrādi veic atšķirīgi, un tādējādi iespējamie riski arī ir atšķirīgi. Ja nevarat objektīvi izvērtēt drošības riskus un izstrādāt rīcības plānu paši, ir vairākas iestādes un organizācijas, kas sniegs konsultācijas atbilstoši jūsu situācijai.

IT drošības incidentu novēršanas institūcija (www.cert.lv)

IT drošības incidentu novēršanas institūcijas (CERT.LV) uzdevumi saskaņā ar Informācijas tehnoloģiju drošības likumu ir uzturēt vienotu elektroniskās informācijas telpā notiekošo darbību atainojumu, sniegt atbalstu informācijas tehnoloģiju drošības incidentu novēršanā vai koordinēt to novēršanu, uzturēt atbilstoši aktuālajiem apdraudējumiem izstrādātas rekomendācijas par aktuālo informācijas tehnoloģiju risku novēršanu, veikt pētniecisko darbu, organizēt izglītojošus pasākumus un apmācības informācijas tehnoloģiju drošības jomā, sniegt atbalstu valsts institūcijām valsts drošības sargāšanā, kā arī noziedzīgu nodarījumu un citu likum-

pārkāpumu atklāšanā. Šajā mājaslapā atradīsit daudz praktiskas informācijas par to, kā veidot savu IT drošības politiku, kā rīkoties incidentu gadījumos un kam lūgt atbalstu.

Datu valsts inspekcija (www.dvi.gov.lv)

Inspekcija sniedz konsultācijas personas datu aizsardzības jautājumos. Uzzināt vairāk varat inspekcijas mājaslapā. Turpat atradīsit arī informatīvus materiālus, rekomendācijas un skaidrojumus par datu aizsardzības un drošības tēmām, kā arī normatīvos aktus – Fizisko personu datu aizsardzības likumu un uz tā pamata izdotos Ministru kabineta noteikumus.

Esi drošs (www.esidross.lv)

Šī mājaslapa ir paredzēta ikvienam, kurš rūpējas par sava datora drošību un savu drošību internetā. Mājas lapu uztur Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (CERT.LV) un tajā informācijas tehnoloģiju speciālisti no Drošības ekspertu grupas sniedz padomus, dalās pieredzē, kā arī ir gatavi atbildēt uz jautājumiem par jūsu datora drošību un jūsu drošību internetā.

Drošs internets (www.drossinternets.lv)

Informācijas resurss, par kura saturu atbild Latvijas Interneta asociācija. Šeit varat atrast gan ieteikumus bērniem, jauniešiem un pieaugušajiem interneta drošai lietošanai, gan arī nozares pētījumus un aptaujas.

Datu valsts inspekcija
Tālr. 67223131
Blaumaņa iela 11/13-15,
Rīga, LV-1011
e-pasta adrese: info@dvi.gov.lv
www.dvi.gov.lv

Telefonkonsultācijas
katru darba dienu laika posmā
no plkst. 13:00-15:00
tālrunis 67223131