DATU VALSTS INSPEKCIJA

Rekomendācija
«Personas datu apstrādes drošība»

Rīga, 2013

Ievads

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 pašā normatīvajā aktā 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.

Drošu un likumdošanai atbilstošu informācijas tehnoloģiju (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 jāpielieto tehniski pasākumi atbilstoši normatīvo aktu prasībām, kā arī Jūsu organizācijas iespējām un vajadzībām. 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.

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

Kāpēc Jums tas vajadzīgs?

Par personas datu apstrādes pārkāpumiem juridiskai personai var piemērot administratīvo sodu līdz pat 10 000 LVL. Gadījumos, kad pārkāpumi konstatēti nolaidības vai ļaunprātības rezultātā, kā arī radīts būtisks kaitējums, iespējama pat krimināltiesiskā atbildība. Turklāt, 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. Novērtējiet, cik vērtīga un konfidenciāla ir informācija, kas ir Jūsu pārziņā, un kādu ietekmi uz konkrētajām personām varētu atstāt tās noplūde drošības incidenta gadījumā. Kad būs apzināts iespējamo risku kopums, varat sākt izvērtēt, kādus Jūsu situācijai atbilstošus drošības pasākumus ieviest.

Valsts un pašvaldību institūcijām saskaņā ar Fizisko personu datu aizsardzības likuma 26. panta otro daļu reizi divos gados jāiesniedz Datu valsts inspekcijai riska analīze, kas ietverta audita atzinumā par personas datu apstrādi. Prasības audita atzinumam par personas datu apstrādi nosaka 2009. gada 17. novembra Ministru kabineta noteikumi Nr.1322 "Prasības audita atzinumam par personas datu apstrādi valsts un pašvaldību institūcijās".

.

Drošības paaugstināšanas pasākumiem 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, kurās glabājas personas dati. Jums jānodrošina, ka personas dati šajās iekārtās ir aizsargāti. Serverus jāizvieto atsevišķās telpās ar pastiprinātu aizsardzību. Rezerves kopiju iekārtas nedrīkst atstāt brīvi pieejamas un nepieskatītas, tās pēc lietošanas jāieslēdz seifā vai jāpārvieto citā drošā vietā.

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

☑ 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.

☑ Aizsardzība pret ārēju ielaušanos

Jūsu 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

Nodrošiniet piekļuvi informācijas sistēmām, kurās ir personas dati, tikai lietotājiem un iekārtām, kurām uzticaties un kuras tām attiecīgi tiek pilnvarotas. Katram lietotājam jāpiešķir savi atšķirīgi autentifikācijas līdzekļi – lietotāja vārds un parole. Sistēmām, kas satur sensitīvus personas datus, būtu jāievieš vairāklīmeņu autentifikācija, piemēram, ar ID kartēm, sertifikātiem, kodu kalkulatoriem vai citiem līdzekļiem.

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.

---

[2] *Ļaunatūra – ļaunprātīga programmatūra (angļu val. –* malware*).*

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

☑ Darbinieku informētības celšana 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.

☑ 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 novēršanu. Efektīvas instrukcijas, plāni un politikas dokumenti būs vērtīgs papildinājums, veicot risku izvērtēšanu un uzlabojot organizācijas pārvaldības procesus kopumā.

☑ 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.

---

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

Datu drošība ārpus biroja

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 uz šīm iekārtām vai nu 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 ar 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, pārsvarā šādu aizsardzību 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 jauninājumus

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

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

Regulāri uzstādiet programmatūras jauninājumus un operētājsistēmas drošības ielāpus. Lielākajai daļai sistēmu iespējams uzstādīt, lai šis process noris automātiski.

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 jautājumos, 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 organizācijas iekšējo informāciju pārsūtot, izmantojot sociālos tīklus vai mākoņpakalpojumus. 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.

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 tiks konstatēta ievainojamība.

Elektroniskā komunikācija starp pakalpojuma sniedzēju un Jums kā pakalpojuma saņēmēju jāšifrē, piemēram, izmantojot uzticamu trešās puses

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

izsniegtu elektronisko sertifikātu. Ieteicams, lai pakalpojumu sniedzēja uzglabātie dati tiktu šifrēti 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 Jūs jānodrošina ar iespēju kontrolēt to, kurš, kad un kādiem datiem piekļūst. Parasti to nodrošina sistēmu auditācijas pieraksti.

Pirms izvēlēties mākoņpakalpojuma sniedzēju, izvērtējiet, vai pakalpojumu sniedzējam būs pietiekami resursi un rezerves jaudas, lai nodrošinātu, ka Jūsu saņemto pakalpojumu neietekmēs pakalpojuma sniedzēja citu klientu noslodze, tādējādi Jūs vienmēr varēsit saņemt pakalpojumu tad, kad tas Jums 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 lauzīsit līgumu ar pakalpojumu sniedzēju, 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 ievainojamību pārbaudes un ielaušanās testus, lai pārbaudītu sistēmu izturību. Nekavējieties ar pretpasākumiem, ja konstatējat nepilnības.

Nosakiet prioritātes

Daudzās organizācijās IT sistēmu aizsardzības līmenis ir nepietiekams tikai tādēļ, ka nav korekti pielietotas esošās drošības procedūras un ka pašas organizācijas nespēj konstatēt, kur un kāpēc var rasties problēmas. Tādēļ ir ne tikai jāizstrādā reāls rīcības plāns 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 raksturīgai 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 sistēmu pārbaudei, lai palīdzētu noteikt, kuri uzlabojumi nepieciešami visvairāk. 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 tās 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 apjoms personas datu, 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, tai skaitā skaidrojot darbiniekiem, kas tiek saprasts ar jēdzienu „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 vēsturiskie dati, kas uzglabājami arhivācijas nolūkiem, un Jums 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.

Kontrolējiet pakalpojumu sniedzējus

Liela daļa nelielu uzņēmumu un organizāciju 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.

---

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

Veiciet neatkarīgu savu personas datu apstrādes sistēmu drošības auditu vai personas datu apstrādes iekšējo auditu, kura rezultātus un turpmākās veicamās darbības izplānojiet kopā ar IT pakalpojumu sniedzēju.

Atcerieties, ka saskaņā ar Ministru kabineta 2001. gada 30. janvāra noteikumu Nr. 40 "Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības" 6.punktu, Jums kā personas datu pārzinim katru gadu jāveic personas datu apstrādes iekšējais audits, kā arī jāsagatavo pārskats par drošības jomā veiktajiem pasākumiem.

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

Neesiet vieglprātīgi pret iekārtu iznīcināšanu – ja lietojat 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.

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 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 no citiem un tādējādi iespējamie riski arī ir atšķirīgi. Ja nevarat objektīvi izvērtēt drošības riskus un izstrādāt rīcības plānu paši, ir vairākas iestādes un organizācijas, kas neatteiks sniegt padomu un 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 likumpārkāpumu 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 Jūsu 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