Rekomendācija

«Personas datu aizsardzība darba vietās»

Rīga

Ievads

„Saglabāt Latvijas cilvēkkapitāla bāzes vērtību un kāpināt tā ražīgumu līdz ES vidējam līmenim, attīstot prasmes, kas sekmē jaunradi, elastību un līdzdalību darba tirgū."[1]

Cilvēkresursi ir ikvienas valsts un arī darba devēja lielākā bagātība, kas ietekmē iespējas sasniegt izvirzītos mērķus gan individuālā, gan nacionālā līmenī. Mūsdienās cilvēkresursu kapitāla attīstību lielā mērā ietekmē informāciju tehnoloģiju un interneta vides attīstība, sekmējot zināšanu sabiedrības attīstības iespējas, uzskatot to par priekšnosacījumu augstai dzīves kvalitātei un nākotnes labklājībai. Cilvēkresursu vadības ietvaros, kā arī darba pienākumu izpildei aizvien biežāk tiek izmantots internets un informāciju tehnoloģijas attiecīgi veicot arī personas datu apstrādi. Izmantojot dažādās informācijas tehnoloģiju un interneta attīstības iespējas, var apstrādāt noteikta apjoma personas datus un tādējādi iespējams ietekmēt personu tiesības uz privātumu.

Šī jautājuma kontekstā ir aktuāls personas datu apstrādes un aizsardzības aspekts, ņemot vērā to, ka personas dati tiek apstrādāti lielā apjomā, mainās datu apstrādes veidi, datu glabāšanas iespējas. Personas datu aizsardzība kļūst par vienu no svarīgākajiem jautājumiem sociālajās attiecībās darba vietās. Indivīda personas datu apstrāde tiek veikta pirms darba tiesisko attiecību nodibināšanas ar konkrēto darba devēju, tā tiek turpināta darba tiesisko attiecību ietvaros, un nereti turpinās arī pēc darba tiesisko attiecību izbeigšanas.

Darba vietās tiek plaši iegūta un izmantota informācija par fiziskām personām (esošiem un potenciālajiem darbiniekiem, klientiem), kā arī tiek lietota videonovērošana un citas tehnoloģijas, lai nodrošinātu darba procesa uzraudzību un darba kvalitātes kontroli. Turklāt darbinieku kontroles ierīces ir savstarpēji saistītas: interneta lietošanas kontrole, elektroniskais pasts, telekomunikācijas, ģeolokācijas ierīces, biometrijas datu apstrāde, videonovērošana, utt. Bez tam, darbinieku atlases procesā un karjeras vadībā darba devēji aizvien palielina dažādu informācijas tehnoloģiju izmantošanu. Ņemot vērā interneta attīstību, personas dati publiski ir pieejami līdz šim nebijušos apmēros, kurus darba devēji izmanto, gan izvērtējot esošos, gan piesaistot potenciālos darbiniekus.

Laikā, kad strauji attīstās viedtālruņu lietošana un kļūst aizvien populārāks attālinātais darbs, ir nepieciešams nodrošināt līdzsvaru starp darbinieku un darba procesa kontroli un privātuma aizsardzību. Šī līdzsvarotība ir saistīta ar katras puses tiesību un pienākumu apzināšanos, kā arī attiecīgu tiesisko ietvaru. Datu valsts inspekcija uzrauga personas datu apstrādi, tai skaitā personas datu apstrādi darba vietās un to aizsardzību. Ņemot vērā minēto un Datu valsts inspekcijas pieredzi, izskatot dažādus iesniegumus un sūdzības, kā arī inidivīdu uzdotos jautājumus konsultāciju laikā un informatīvajos semināros, Datu valsts inspekcija ir sagatavojusi rekomendāciju attiecībā uz personas datu apstrādi un to aizsardzību darba vietās ar mērķi motivēt darba devējus pārdomāt dažādus personas datu aizsardzības un datu apstrādes jautājumus, lai kopumā uzlabotu datu aizsardzību

1 Latvijas ilgtspējīgas attīstības stratēģija līdz 2030.gadam. Mērķis – Ilgtermiņa ieguldījumi cilvēkkapitālā,17.lpp. Skatīt – http://www.pkc.gov.lv/images/LV2030/Latvija_2030.pdf.

darba vietās. Šī rekomendācija ir sagatavota ar mērķi palīdzēt nodrošināt personas datu apstrādes atbilstību Fizisko personu datu aizsardzības likumam.

Fizisko personu datu aizsardzības likums attiecas uz jebkuru darbību (apstrādi) ar jebkādu informāciju par dzīvām, identificējamām fiziskām personām (darba tiesiskās attiecībās – pretendenti, klienti un darbinieki). Ņemot vērā personas datu aizsardzības principus, Fizisko personu datu aizsardzības likums nosaka, kā informāciju par personām var vākt, glabāt un izmantot. Likums paredz personas tiesības saņemt atlīdzību, ja viņa personas datu apstrāde nav veikta saskaņā ar likumu un tādējādi personai ir nodarīts kaitējums vai radīti zaudējumi. Likums attiecas gan uz elektroniski apstrādātu informāciju, gan uz manuāli (rakstveidā) apstrādātiem datiem, piemēram, tādiem kā dažādiem dokumentiem, kurus iesniedz pretendents, gan citādā formātā apstrādātiem datiem (piemēram, mutvārdos veikta apstrāde).

Rekomendācija sniedz tikai ieskatu svarīgākajos personas datu apstrādes un aizsardzības darba vietās aspektos, un katram darba devējam (pārzinim) ir jāvērtē, kādam mērķim un kādā apjomā veikt personas datu apstrādi, kā arī ir jāizvērtē drošības pasākumi katrā konkrētajā situācijā, lai nodrošinātu personas datu aizsardzību.

Eiropas Savienībā nav speciāla ES tiesību akta, kas attiektos tieši uz darbinieku personas datu apstrādi un aizsardzību, bet jāņem vērā Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi. Rekomendācija ir izstrādāta, ņemot vērā Direktīvas 95/46/EK 29. panta datu aizsardzības darba grupas apstiprināto atzinumu Nr.8/2001 „Personas datu apstrāde nodarbinātības jomā" un darba dokumentu Nr.55 (2002. g.) „Elektroniskās komunikācijas novērošana darba vietā"[2], kā arī ņemot vērā Datu valsts inspekcijas un Eiropas Savienības dalībvalstu iestāžu, kuras uzrauga personas datu aizsardzību, pieredzi.

2 Rekomendāciju tekstus skatīt – http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

Personas datu aizsardzība ir sarežģīta joma, tādēļ ikvienam darba devējam būtu jāizvērtē, vai nav nepieciešams nozīmēt noteiktu personu, kuras pienākumos būtu organizēt, kontrolēt un uzraudzīt darba devēja veiktās personas datu apstrādes atbilstību likuma prasībām. Darba devējam nepieciešams nodrošināt šīs personas regulāru apmācību personas datu aizsardzības jautājumos. Svarīgi jebkuru darbinieku, kura pienākumos ietilpst personas datu apstrāde, apmācīt jautājumos, kas skar personas datu aizsardzību. Tā, piemēram, arī veikala darbiniekam nepieciešams zināt, kādi dati par klientiem un kādam mērķim tiek vākti, lai klientiem sniegtu informāciju par viņu personas datu apstrādi.

Darba devējiem, veicot personas datu apstrādi un aizsardzību, nepieciešams atcerēties, ka darbinieks nezaudē savas tiesības uz privātuma aizsardzību un personas datu aizsardzību arī tad, kad ir kļuvis par darba ņēmēju pie konkrēta darba devēja. Jebkādiem šo abu tiesību ierobežojumiem ir jābūt likumīgiem, samērīgiem un proporcionāliem.

I. Darba tiesisko attiecību nodibināšana

Darba tiesiskās attiecības regulē Latvijas Republikas Satversme, Latvijai saistošās starptautisko tiesību normas, šis likums un citi normatīvie akti, kā arī darba koplīgums un darba kārtības noteikumi. Savukārt Darba likums un citi normatīvie akti, kas regulē darba tiesiskās attiecības, ir saistoši visiem darba devējiem neatkarīgi no to tiesiskā statusa un darbiniekiem, ja darba devēju un darbinieku savstarpējās tiesiskās attiecības dibinātas uz darba līguma pamata.

Valsts darba inspekcija uzrauga un kontrolē darba tiesisko attiecību un darba aizsardzības normatīvo aktu prasību ievērošanu (saskaņā ar Valsts darba inspekcijas likumu). Kā arī kontrolē, kā darba devēji un darbinieki savstarpēji pilda darba līgumos un darba koplīgumos noteiktos pienākumus. Turklāt Valsts darba inspekcija konsultē darba devējus un darbiniekus par darba tiesiskajām attiecībām un darba aiz-

sardzību, veicina sabiedrības izpratni par darba tiesību un darba drošības normu ievērošanas nozīmību.

Veicot potenciālo darbinieku atlasi, darba devēji un personas, kas veic darbinieku atlasi (personāla atlases uzņēmumi), bieži izmanto informācijas tehnoloģijas un datu bāzes, kas ir pašu darba devēju rīcībā, vai tiek izmantoti ārpakalpojumu sniegtie pakalpojumi. Izmantojot tās, personas dati tiek apkopoti, analizēti, un attiecīgi informācijas sistēmas un informācijas tehnoloģiju ierīces satur daudz personas datus par pretendentiem un darbiniekiem. Kāda informācija var tikt izmantota? Kādiem mērķiem? Cik ilgi var uzglabāt personas datus? Kādas darbības ar personas datiem ir aizliegtas?

Ar jaunu rindkopu - Vēršam uzmanību, ka individuāli tiesību strīdi starp darbinieku un darba devēju, ja tie nav izšķirti uzņēmumā, izšķirami tiesā.

Kādu informāciju var vākt un ko ar to var darīt?

Pārliecinieties, ka, izvietojot darba sludinājumu, jūs identificējat savu organizāciju vai uzņēmumu atbilstoši – personām ir jāzina, kam tās nosūta savus datus. Ja izmantojat personāla atlases uzņēmumu palīdzību, pārliecinieties, ka tas sevi identificē.

Darbinieku atlases procesā iegūtos personas datus var izmantot tikai, lai novērtētu iespējamību pretendentam ieņemt noteiktu amatu (kvalifikācija, pieredze, utt.), un nedrīkst pieprasīt informāciju, kas neattiecas uz paredzētā darba veikšanu vai nav saistīta ar pretendenta piemērotību šim darbam.

No pretendenta ir aizliegts pieprasīt tādu informāciju, kas nav nepieciešama, lai izvērtētu viņa/viņas atbilstību amatam (piemēram, personas kodu, dzimšanas datumu), tostarp, jāievēro tie ierobežojumi, kas noteikti Darba likuma 33. panta otrajā daļā (t.i., aizliegts prasīt informāciju par grūtniecību, ģimenes vai laulības stāvokli, iepriekšēju sodāmību (izņemot gadījumus, kad tam attiecībā uz veicamo darbu varētu būt būtiska nozīme), reliģisko pārliecību vai piederību pie kādas reliģiskās konfesijas, piederību pie kādas politiskās partijas, darbinieku arodbiedrības vai citas sabiedriskās organizācijas, nacionālo vai etnisko izcelsmi).

Rekomendējam sagatavot speciālas formas, kurās pretendenti varētu sniegt informāciju par savu dzīvesgājumu (Curriculum Vitae), un izstrādāt procedūru, kādā pretendenti sagatavo un iesniedz šo informāciju darba devējam vai personāla atlases uzņēmumam. Tas nodrošinās, ka tiks apstrādāti tikai tie personas dati, kas nepieciešami mērķa sasniegšanai, tie tiks precīzi definēti un tiks adekvāti ieviesti nepieciešamie aizsardzības līdzekļi.

Darba likums paredz darba devēja tiesības pieprasīt informāciju par pretendenta veselības stāvokli, ja tai ir būtiska nozīme darba līguma noslēgšanā un paredzētā darba veikšanā. Darba likums nosaka arī, ka darba devējs var pieprasīt, lai pretendents veic veselības pārbaudi, kas ļautu pārliecināties par viņa piemērotību paredzētā darba veikšanai, saskaņā ar Ministru kabineta 2009. gada 10. marta noteikumiem Nr.219 „Kārtība, kādā veicama obligātā veselības pārbaude". Atzinumā par personas veselības stāvokli arodslimību ārsts sniedz izvērtējumu un atzinumu par indivīda veselības stāvokļa atbilstību veicamajam darbam.

Ir aizliegts vākt informāciju (ja vien tā specifiski un tieši nav saistīta ar vakanto amatu) par pretendenta vecākiem, citiem radiniekiem (māsām, brāļiem, u.c.), naturalizācijas laiku, procedūru, kādā ir iegūta Latvijas Republikas pilsonība, informāciju par veselību (ja vien tā nav informācija par veselību, kurai ir būtiska nozīme darba līguma noslēgšanā un paredzētā darba veikšanā; Darba likuma 33. panta ceturtā daļa), garumu, svaru, izskatu, informāciju par filozofisko un politisko pārliecību, informāciju par personas seksuālo dzīvi, par īpašumiem, dalību dažādās asociācijās, kredītinformāciju, kredītvēstures informāciju, parādiem un informāciju par sodāmību (gan administratīvo, gan kriminālo). Turklāt personas piekrišana iepriekš minēto personas datu ievākšanai nevar tikt uzskatīta par tiesisko pamatu, ja vien šāda datu vākšana nav īpaši saistīta ar vakanto amatu. Savukārt, ja konkrētās informācijas par pretendentu pieprasīšana ir paredzēta likumā (piemēram, saskaņā ar likumu konkrētus amatus konkrētās iestādēs nedrīkst ieņemt personas, kas sodītas par noteiktiem pārkāpumiem), tad šo informāciju likumā noteiktajā apjomā un gadījumā darba devējam ir tiesības iegūt bez pretendenta piekrišanas.

Iegūt informāciju no pretendenta iepriekšējām darba vietām, atsauksmes no tām (kolēģiem, vadītājiem, u.c.) ir atļauts, ja pretendents tam ir iepriekš devis savu piekrišanu (ieteicams formulētu rakstiski, lai strīdus gadījumā pārzinis varētu pierādīt, ka šāda piekrišana ir bijusi).

Pieņemot darbā darbinieku, darba devējs var ievākt (apstrādāt) papildu informāciju (personas datus). Papildus informācijai, kas nepieciešama, lai nodrošinātu atbilstību normatīvajiem aktiem (piemēram, slēdzot līgumu par darba tiesiskajām attiecībām ir nepieciešams dzimšanas datums, personas kods), darba devējs var vākt arī šādu nepieciešamo informāciju:

- personālvadības mērķiem (piemēram, autovadītāja atļaujas veidu, personas kontaktinformāciju saziņai ārkārtas gadījumos);

- darba organizācijas mērķiem (piemēram, fotogrāfija priekš iekšējiem organizācijas vai uzņēmuma darbinieku sarakstiem) kā neobligāta prasība;

- sociālo garantiju nodrošināšanas mērķiem (piemēram, informācija par darbinieka apgādībā esošajām personām).

Attiecībā uz internetā pieejamiem resursiem, kuros ir izvietota informācija par personām, kas meklē darbu, šo interneta resursu uzturētājiem ir jāinformē pretendenti, pirms personas publicē informāciju par sevi, kā viņu personas dati tiks izplatīti, t.i., tiks izvietoti tiešsaistē vai tiks nosūtīti noteiktiem darba devējiem, citām trešajām personām, kā arī cik ilgi tiks saglabāti konkrētajā interneta vietnē.

Kas var piekļūt personas datiem?

Personas datiem var piekļūt tikai tās personas, kas ir iesaistītas darbinieku atlases procesā. Administratīvie darbinieki, kas nodrošina personāla vadību, ir tiesīgi piekļūt tikai tai informācijai par darbinieku, kas saistīta ar to tiešajiem darba pienākumiem: darbinieku apdrošināšana, sociālās garantijas, darba nespēja, darba attiecību izbeigšana, utt.

Darbinieki, kas saistīti ar kāda konkrēta darbinieka darba pienākumu izpildi, var iegūt tikai to informāciju par šo darbinieku, kas saistīta ar savu funkciju

izpildi (piemēram, darbinieku novērtēšanas informācija u.c.).

Darba devējs nav tiesīgs izpaust darbinieka personas datus, ja vien tas nav noteikts likumā (piemēram, atsevišķām valsts iestādēm saskaņā ar rakstveida pieprasījumu) vai nav nepieciešams darba līguma un darbinieka interešu ievērošanai (piemēram, ja darbinieks piekrīt un vēlas izmantot darba devēja piedāvāto veselības apdrošināšanu, tad darba devējs ir tiesīgs noteikta apjoma darbinieka personas datus nodot apdrošināšanas sabiedrībai apdrošināšanas polises sagatavošanai).

Pretendentiem nav tiesības iegūt citu pretendentu personas datus. Darba likums nosaka, ka ziņas par pretendentu un darbā pieteikšanās dokumentus drīkst darīt zināmus trešajām personām tikai ar pretendenta piekrišanu.

Kontrolēta pieeja datiem

Darba devējam ir jānodrošina informācijas aizsardzība, drošība un jānodrošina, ka tikai attiecīgi pilnvaroti tā darbinieki var piekļūt noteiktiem personas datiem. Visām darbībām ar personas datiem (tai skaitā arī skatīšanās režīms, datu iegūšana, izmantojot sistēmā meklēšanas funkciju) ieteicams būt uzskaitītām (piemēram, ar auditācijas pierakstu palīdzību), jo pārzinim ir pienākums nodrošināt iespēju noteikt personas datus, kuri bijuši apstrādāti bez attiecīgā pilnvarojuma, kā arī apstrādes laiku un personu, kas to veikusi.

Kādi ir darba devēja pienākumi personas datu aizsardzībā?

Tiesības būt informētam

Darba devējam ir pienākums informēt darbiniekus pirms viņu personas datu ievākšanas. Fizisko personu datu aizsardzības likuma 8. pants nosaka, ka, iegūstot personas datus no datu subjekta (piemēram, darbinieka), pārzinim ir pienākums sniegt datu subjektam šādu informāciju, ja vien tā jau nav datu subjekta rīcībā: pārziņa un personas datu operatora nosaukums vai vārds un uzvārds, kā arī adrese, paredzētais personas datu apstrādes mērķis un pamatojums.

Pēc datu subjekta pieprasījuma pārzinim ir pienākums sniegt arī šādu informāciju: iespējamie personas datu saņēmēji, datu subjekta tiesības piekļūt saviem personas datiem un izdarīt tajos labojumus, vai datu subjekta atbildes sniegšana ir obligāta vai brīvprātīga, kā arī iespējamās sekas par atbildes nesniegšanu.

Pretendentiem un darbiniekiem jābūt informētiem par:

- atbildīgo par personas datu apstrādi – pārzini un personas datu operatoru (tai skaitā personāla atlases uzņēmumi);

- konkrētiem un skaidriem personas datu apstrādes mērķiem.

Lai nodrošinātu personas datu godprātīgu apstrādi, rekomendējam pretendentiem un darbiniekiem sniegt arī šādu informāciju:

- vai informācijas sniegšana ir obligāta vai brīvprātīga, un kādas būs sekas, ja informācija netiks sniegta;

- personas datu avoti (piemēram, citi personāla atlases uzņēmumi);

- tiesības izmantot savas tiesības, ko nosaka likums (tādas kā pieejas tiesības saviem datiem un tiesības izdarīt labojumus savos datos).

Ja pretendents nosūta savu pieteikumu, dzīvesgājuma aprakstu (CV) un citus dokumentus, rekomendējam informāciju par pārzini, personas datu operatoru un personas datu apstrādes mērķi nosūtīt konkrētajam pretendentam, apstiprinot viņa elektroniskā pasta sūtījuma saņemšanu. Ja pretendents iesniedz dokumentus personīgi, tad šī informācija viņam jāsniedz klātienē, un ieteicams saglabāt pierādījumus, ka šī informācija ir sniegta.

Pretendentam ir tiesības saņemt informāciju par personālatlases metodēm, kas tiks izmantotas personālatlasē, apstrādājot personas datus. Nevar tikt vākta informācija par pretendentu, ja tas pirms tam nav bijis informēts par viņa personas datu iegūšanu. Tas pats attiecas arī uz izmantotajiem tehniskajiem līdzekļiem un metodēm.

Personas datu saglabāšanas ilgums

Ja pretendents nav ticis pieņemts darbā, tad darba devējam ir pienākums informāciju par pretendentu iznīcināt, jeb dzēst pēc tam, kad personālatlase uz noteikto amatu ir pabeigta un ir pagājis termiņš lēmuma pārsūdzēšanai. Ja darba devējs vēlas saglabāt informāciju par pretendentu iespējamai turpmākai personālatlasei uz citiem amatiem, ir jāprasa pretendenta piekrišana datu uzglabāšanai.

Personas dati ir jāglabā, ievērojot vispārīgās datu glabāšanas un drošības prasības, tai skaitā ar tehniskiem un organizatorisiem līdzekļiem jānodrošina, ka personas datiem nepiekļūst nepilnvarotas personas.

Pretendenta datu turpmāka apstrāde, neskaitot iepriekš minētos izņēmumus (pārsūdzēšanas termiņš un turpmāka personālatlase uz citiem amatiem), ir pieļaujama tikai, ja tiek noslēgts darba līgums. Darba devējs var uzglabāt datus par darbinieku, ja ar to ir darba tiesiskās attiecības.

Saskaņā ar normatīvajiem aktiem darba devējam noteikta veida informācija par darbinieku ir jāsaglabā arī pēc darba tiesiskajām attiecībām, lai to nodotu arhīvā (vēsturiskiem mērķiem). Saskaņā ar Arhīvu likumu dokumentus par personas darba vai dienesta gaitu glabā 75 gadus.

Darba devējam var būt nepieciešams informāciju par darbinieku saglabāt arī pēc darba tiesisko attiecību beigām, arī lai atrisinātu strīdus, ja tādi ar darbinieku rodas pēc darba tiesisko attiecību izbeigšanas.

II. Personāla dokumenti

Veidojot darbinieku personas lietas, ir jāievēro Fizisko personu datu aizsardzības likumā noteiktais. Informācija, kas iekļauta personas lietās, nevar tikt izmantota citiem mērķiem nekā tā sākotnēji ievākta, piemēram, komerciāliem vai politiskiem mērķiem.

Attiecībā uz dažādu darba apstākļu izmaiņu ieviešanu (piemēram, videonovērošanu, pieejas kontroles sistēmām, būtisku personas datu apstrādes un aizsardzības apstākļu maiņu), saskaņā ar Darba likuma 11. pantu, darbinieku pārstāvjiem ir tiesības savlaicīgi saņemt informāciju un konsultēties ar darba devēju pirms darba devējs pieņem tādus lēmumus, kas var skart darbinieku intereses un darba apstākļus, darba vidi un darbinieku drošības aizsardzību, kā arī uzraudzīt, kā darba tiesiskajās attiecībās tiek ievēroti normatīvie akti, tai skaitā Fizisko personu datu aizsardzības likums.

Kādus datus var vākt darba devējs?

Darba devējs var apstrādāt tikai tādus personas datus par darbiniekiem, kas ir atbilstoši noteiktam mērķim (t.i., darba tiesisko attiecību nodibināšanai, nodrošināšanai vai izbeigšanai), nav pārmērīgi, un darba devējs ir atbildīgs par personas datu pareizību un to savlaicīgu atjaunošanu, labošanu vai dzēšanu. Darba devējam jādzēš tie dati, kas nav nepieciešami tiesiska mērķa sasniegšanai vai tos saglabāt neprasa atbilstoši normatīvie akti, tai skaitā arhīvu jomā.

Datu valsts inspekcija iesaka personas attēlus saglabāt personas lietā tikai ar personas iepriekšēju piekri-

šanu, it īpaši, ja plānots fotogrāfiju izvietot publiski vai internetā.

Tiesības būt informētam

Darba devējam ir ieteicams informēt darbiniekus pirms personas lietas izveidošanas (jeb personas datu vākšanas), par pieejas tiesībām saviem personas datiem, tiesībām labot vai precizēt informāciju vai iebilst pret informācijas sniegšanu.

Personas datu glabāšana

Iesakiet un atļaujiet darbiniekam periodiski pārbaudīt informāciju savā personas lietā, jo tādējādi darba devējs var izvairīties no neaktuālas informācijas glabāšanas. Nodrošiniet, ka personāla dokumenti tiek glabāti droši. Glabājiet papīra dokumentus slēgtās telpās vai skapjos, vai lietojiet paroles, ja informācija tiek glabāta elektroniski. Pārliecinieties, ka personālam, kas var piekļūt personāla dokumentiem, ir attiecīgas pieejas tiesības, nepieciešamās zināšanas un tiek veikta personāla atbilstoša apmācība, lai nodrošinātu atbilstošu pieeju personāla dokumentiem un to aizsardzību.

Ja iespējams, glabājiet informāciju par darbinieku veselības stāvokli atsevišķi no mazāk sensitīvas informācijas, piemēram, saglabājot tikai ierakstu, ka darbinieks ir bijis prombūtnē, kā arī izvērtējiet šādas informācijas glabāšanas termiņu. To var nodrošināt, saglabājot informāciju par darbinieka veselības stāvokli slēgtā aploksnē vai aizsargāta datora failā. Atļaujiet piekļūt šai informācijai tikai tiem darbiniekiem, kuriem tas tiešām ir nepieciešams, veicot darba pienākumus.

Ja jūsu rīcībā ir sensitīvi personas dati (personas dati, kas norāda rasi, etnisko izcelsmi, reliģisko, filozofisko un politisko pārliecību, dalību arodbiedrībās, kā arī sniedz informāciju par personas veselību vai seksuālo dzīvi), un tos paredzēts apstrādāt, lai nodrošinātu un uzraudzītu vienlīdzīgu tiesību principa (Darba likuma 7. pants) ievērošanu (piemēram, darbiniekiem ar invaliditāti, neatkarīgi no personas rases, ādas krāsas, dzimuma, vecuma, reliģiskās, politiskās vai citas pārliecības, nacionālās vai sociālās izcelsmes, mantiskā vai ģimenes stāvokļa, seksuālās orientācijas vai citiem apstākļiem), izmantojiet nepieciešamo informāciju tikai šī mērķa sasniegšanai.

Ja iespējams, izmantojiet šo informāciju tikai anonimizētā formā, lai nepieļautu noteikta darbinieka identifikāciju.

Piekļuve personāla dokumentiem

Darba devējam ir jānodrošina, ka personas, kam ir tiesības piekļūt personāla dokumentiem, pārzina personas datu aizsardzības noteikumus, kas šajos dokumentos esošajai informācijai ir jāpiemēro, un šī informācija jeb personas dati tiek attiecīgi aizsargāti. Pirms personāla dokumentu izpaušanas vai nodošanas citām personām (tai skaitā citiem darbiniekiem) pārliecinieties, vai tam ir tiesiskais pamats un likumīgs mērķis.

Nodrošiniet, ka darbinieku personas dati netiek nodoti citām personām, ja vien pats darbinieks tam iepriekš nav piekritis (lai par to pārliecinātos, pārjautājiet to attiecīgajam darbiniekam), vai šādu prasību nenosaka ārējie normatīvie akti. Fizisko personu datu aizsardzības likuma 13. pants nosaka, kādos gadījumos un kādā veidā no darba devēja var saņemt per-

sonas datus valsts un pašvaldību amatpersonas (t.sk. policijas amatpersonas).

Dažādu informācijas sistēmu izmantošana, lai apstrādātu darbinieku personas datus

Nereti darbinieku atalgojuma un personāla dokumentu apstrādei, kā arī darbinieku un darba devēja īpašuma aizsardzības nodrošināšanai tiek izmantotas informācijas sistēmas (piemēram, videonovērošanas sistēmas), kuras uztur ārpakalpojumu sniedzēji. Šiem uzņēmumiem attiecīgi ir pieeja darbinieku personas datiem, un saskaņā ar Fizisko personu datu aizsardzības likumu šie uzņēmumi ir uzskatāmi par personas datu operatoriem. Ar šiem uzņēmumiem ir jābūt noslēgtiem attiecīgiem līgumiem, kā to nosaka Fizisko personu datu aizsardzības likuma 14. panta pirmā un otrā daļa. Līgumos ir jābūt noteiktam personas datu apjomam, datu apstrādes mērķim un pārziņa norādījumiem attiecībā uz apstrādi. Šajos līgumos vai citā dokumentā tostarp ir jābūt noteiktiem datu drošības pasākumiem, kas jāveic personas datu apstrādes operatoriem pirms apstrādes uzsākšanas un līguma darbības laikā.

III. Personas datu nodošana uz citām valstīm

Personas datus uz citām valstīm var nodot, izmantojot internetu, elektronisko pastu, cita veida elektroniskos tīklus, kurjeru, utt. Piemēram, centralizēta personālvadības sistēma, kas atrodas citā valstī, personas datu glabāšana serveros, kas atrodas citās valstīs, personas datu ievadīšana sistēmās, kas atrodas citās valstīs, utt.

Lai nodotu personas datus ārpus Latvijas Republikas, ir jābūt skaidri noteiktam un likumiskam mērķim. Pārzinim ir jāsniedz datu subjektiem informācija, kam tiks nodota informācija par datu subjektu (kas ir personas datu operators vai cits pārzinis, kuram personas dati tiek nodoti) un kāpēc (mērķis) personas dati tiks nodoti (tai skaitā datu nodošana mātes kompānijai, datu glabāšanai ārpus Latvijas Republikas, izmantojot ārpakalpojumus, u.c.) un pirms personas datu nodošanas pārzinim jāpārliecinās, ka šādai personas datu nodošanai pastāv tiesiskais pamats saskaņā ar Fizisko personu datu aizsardzības likumu (likuma 28. pants).

Personas datu nodošanai un tās ietvaros nododamo datu apjomam ir jābūt proporcionālam, saistītam un ne pārmērīgam attiecībā uz datu nodošanas jeb datu apstrādes mērķi, saistībā ar kuru tie tiek nodoti uz citām valstīm. Papildus informāciju par personas datu nodošanu uz citām valstīm ir iespēja iegūt Datu valsts inspekcijas rekomendācijā „Personas datu nodošana uz citām valstīm" (http://www.dvi.gov.lv/fpda/).

Attiecībā uz personas datu nodošanu viena koncerna ietvaros rekomendējam darba devējam izvērtēt, vai nepieciešams nodot visus darbinieku datus, kas ir konkrētā darba devēja rīcībā, citiem uzņēmumiem vai sabiedrībām, kas ietilpst koncernā, vai arī pietiekama ir mazāka personas datu apjoma nodošana.

IV. Sistēmas, kas nodrošina darbiniekiem iespēju ziņot par dažādiem pārkāpumiem

Darba devēji nereti ievieš speciālas darbinieku ziņošanas sistēmas, kuras izmantojot, darbiniekam ir iespējams ziņot par dažādiem pārkāpumiem organizācijā vai uzņēmumā, tai skaitā arī par auditoru darbību, ko reglamentē dažādu valstu normatīvie akti. Līdz ar to ir jāvērtē arī personas datu apstrādes aspekti saistībā ar personas datu nodošanu uz trešajām valstīm.

Speciālās darbinieku ziņošanas sistēmas parasti ir tiešsaistes sistēmas, piemēram, īpašas elektroniskā pasta adreses, uz kurām darbinieks var nosūtīt informāciju par iespējamo pārkāpumu. Šādu sistēmu ieviešanai un uzturēšanai ir jābūt tiesiskajam pamatam saskaņā ar Fizisko personu datu aizsardzības likumu (likuma 7. pants). Darbiniekiem ir jābūt informētiem par šādu sistēmu pastāvēšanu. Ja personas dati saistībā ar anonīmo ziņojumu tiek nosūtīti izmeklēšanai trešajām personām, tad iesaistītās personas (datu subjekti) ir nekavējoties jāinformē par datu nosūtīšanu (gan vienas organizācijas vai uzņēmuma ietvaros, gan saistībā ar datu nodošanu uz citām valstīm), ja vien to neaizliedz likums.

Šo sistēmu kontekstā ir jānodrošina arī proporcionalitātes princips (likuma 10. panta pirmās daļas 2. punkts), tai skaitā, darba devējam iekšējās procedūrās ir jānosaka, par kādiem pārkāpumiem darbinieki var ziņot, tādējādi jau sākotnēji ierobežojot apstrādājamo personas datu apjomu.

Lai veicinātu personas datu pareizību un precizitāti (un mazinātu nepatiesu sūdzību iesniegšanu), darba devējam ir ieteicams izstrādāt procedūras, kas nosaka, ka tiek akceptētas tikai tādas sūdzības, kurās ir iespējams identificēt tās iesniedzēju. Sistēmas, kas paredzēta anonīmai ziņošanai par pārkāpumiem, ieviešana nav atbalstāma. Visos gadījumos ir jānodrošina, ka sūdzības iesniedzēja identitāte ir konfidenciāla, un netiek izpausta personai, par kuru tiek iesniegta sūdzība. Vienlaicīgi ir jānodrošina arī atbilstošs personas datu glabāšanas termiņš.

V. Informācijas tehnoloģiju izmantošana darba vietās

Kā tika norādīts iepriekš, informācijas tehnoloģiju izmantošana darba vietās kļūst aizvien plašāk izplatīta. Darba devēja tiesības un pienākums ir noteikt ierobežojumus to izmantošanai un attiecīgi informēt par to darbiniekus.

Interneta un elektroniskā pasta kontrole: kādiem mērķiem?

Darba devējs var kontrolēt un ierobežot interneta izmantošanu (tai skaitā, noteikt konkrētu interneta lapu, kaitīgo programmatūru lietošanas aizliegumu, utt.) un saziņas līdzekļu izmantošanu (tai skaitā, sūtījumu apjoma noteikšana, "spam" filtri, utt.).

Šī kontrole paredzēta, lai darba devējs:

- nodrošinātu tīklu drošību atbilstoši apdraudējumiem (dažāda veida kaitīgās programmatūras, u.c.);

- samazinātu risku pieļaut pārmērīgu interneta lietošanu un saziņas līdzekļu lietošanu personīgiem mērķiem (preču iegāde, ceļojumi, diskusijas sociālajos tīklos, u.c.).

Kādi ir pienākumi personas datu aizsardzībā?

Darba devēja ierobežojumi kontrolēt darbiniekus:

- Darba devējs nevar saņemt automātiskas kopijas no visām saņemtām un nosūtītām darbinieka elektroniskā pasta vēstulēm. Tas ir pārmērīgi.

- Darba devējs nedrīkst saglabāt informāciju par visām darbībām, ko darbinieks veic ar datoru. Izņēmums – ja pie noteiktiem nosacījumiem ir nepieciešams nodrošināt īpaši augsta līmeņa drošības aizsardzību. Pretējā gadījumā šāda veida darbinieku darbību monitorēšana ir nelikumīga.

- Servera auditācijas pierakstus var saglabāt noteiktu laiku.

Elektroniskā pasta aizsardzība

Darbiniekam pat darba vietā ir tiesības, uz tā privātās koresondences privātumu un konfidencialitātes res-

pektēšanu. Darba devējs nedrīkst brīvi lasīt darbinieku elektroniskā pasta sūtījumus, pat ja tiek lietotas darba devēja ierīces.

Darba devējs var noteikt, ka darbinieks nevar izmantot tam piešķirto elektroniskā pasta adresi, lai nosūtītu privātus elektroniskā pasta sūtījumus.

Sūtījumos, ko darbinieks sūta no darba devēja piešķirtās elektroniskā pasta adreses, darba devējs var ieviest automātisku norādi, ka šī ir darba devēja elektroniskā pasta adrese.

Lai aizsargātu privātos elektroniskā pasta sūtījumus, darbiniekam nepieciešams tos skaidri iezīmēt ar norādi „Privāts", vai arī darbiniekam tie nekavējoties jāizdzēš.

Darbiniekam ir jāsaglabā visa informācija, kas nepieciešama darbam, resursos, kas ir pieejami darba devējam vai citiem darbiniekiem.

Darba devējam būtu jānozīmē persona, kam tiek pārsūtīti prombūtnē esošā darbinieka elektroniskā pasta sūtījumi. Šajā gadījumā prombūtnē esošajam darbiniekam iepriekš ir jādod piekrišana tā elektroniskā pasta sūtījumu atvēršanai viņa prombūtnes laikā.

Tomēr, ja darbinieks ir prombūtnē un darbinieka rīcībā esošā informācija ir nepieciešama, lai izpildītu noteiktās funkcijas un uzdevumus, darba devējs var pieprasīt administratoram piekļuvi elektroniskajam pastam.

Vēstules nevar tikt uzskatītas par personisku informāciju tikai tāpēc, ka tās ir saglabātas datorā direktorijā „Mani dokumenti" (My Documents) vai fails satur darbinieku identificējošu informāciju.

Privātu elektroniskā pasta sūtījumu aizsardzība netiek nodrošināta, ja notiek kriminālprocess (piemēram, ja darbinieks ir aizdomās turētais par kompā-

nijas komercnoslēpumu izpaušanu, u.tml.) vai, ja darba devējam ir pamatotas aizdomas par darbinieka iespējamu likumpārkāpumu, par kuru paredzēta kriminālatbildība. Šādu līdzekļu izvēlē darba devējam ir pienākums ievērot proporcionalitātes principu. Darbiniekam ir tiesības iesniegt sūdzību par pārbaudes veikšanu Datu valsts inspekcijā.
Ne vienmēr ir nepieciešams pēc darba tiesisko attiecību izbeigšanas saglabāt darbinieka elektronisko pastu aktīvu, jo darba devējs var izveidot automātisku atbildi, kas informē, ka noteiktā elektroniskā pasta adrese ir slēgta un ir jauna kontaktinformācija saziņai ar darba devēju.

Darbiniekam pēc darba tiesisko attiecību izbeigšanas ir jāsaglabā un jādara pieejama darba devējam visa elektroniskā pasta korespondence, kas attiecas uz tā darba pienākumu veikšanu.

Datu faili

Pēc noklusēšanas datu failiem ir profesionāls raksturs un darba devējs var tiem brīvi piekļūt., kā arī noteikt savu informācijas tehnoloģiju resursu izmantošanas kārtību.

Ja datu failus darbinieks ir identificējis kā „personiski", darba devējs var tiem piekļūt:

- ar darbinieka atļauju un tā klātbūtnē;

- ja darba devējam ir pamatotas aizdomas par darbinieka iespējamu likumpārkāpumu, par kuru paredzēta kriminālatbildība. Šādu līdzekļu izvēlē darba devējam ir pienākums ievērot proporcionalitātes principu.

Paroles

Lietotājvārdi un paroles ir konfidenciālas un nevar tikt nodotas darba devējam. Tomēr, ja darbinieks ir prombūtnē un darbinieka rīcībā esošā informācija ir nepieciešama, lai izpildītu noteiktās funkcijas un uzdevumus, darba devējs var pieprasīt administratoram pieejas datus. Katra darbinieka pienākums ir glabāt darba devēja piešķirtās paroles tā, lai tām nepiekļūtu personas, kam nav tiesības tām piekļūt, tostarp citi darbinieki, un tā, kā to ir noteicis darba devējs.

Darbiniekam sniedzamā informācija

Darbiniekiem jābūt informētiem par personas datu apstrādes mērķiem un pamatojumu.

Lai nodrošinātu personas datu godprātīgu apstrādi, rekomendējam informēt darbiniekus arī par:

- iespējamiem personas datu saņēmējiem;

- tiesībām izmantot savas tiesības, ko nosaka likums (piemēram, pieejas tiesības saviem datiem un tiesības izdarīt labojumus savos datos).

Darbinieka informēšanai ir jābūt noformētai skaidri, nepārprotami un saprotami. Iesakām to noformēt kā atsevišķu dokumentu, nevis iekļaut vai pievienot vispārējiem noteikumiem organizācijā vai uzņēmumā.

VI. Videonovērošana darba vietās

Darba vietas aizvien vairāk tiek aprīkotas ar videonovērošanas ierīcēm. Tās ir likumīgas, ja ar to palīdzību tiek nodrošināta cilvēku dzīvības, veselības aizsardzība un īpašuma aizsardzība, bet tās nevar tikt izmantotas, lai darbiniekus patstāvīgi un ilgstoši novērotu un kontrolētu. Personas datu apstrāde, veicot videonovērošanu, var tikt veikta pat tad, ja datu subjekta (t.sk. pretendenta, darbinieka, klienta) seja nav saskatāma videonovērošanas attēlā, kā arī ja videonovērošana notiek tikai reālajā laika režīmā vai arī tiek veikta videonovērošanas ieraksta saglabāšana).[3]

Kādiem mērķiem?

Videonovērošanas ierīces var būt izvietotas darba vietās, lai nodrošinātu cilvēku dzīvības, veselības aizsardzību un īpašuma aizsardzību, lai identificētu kaitējumu vai zaudējumu nodarītājus. Videonovērošanas ierīču ieraksti nevar tikt izmantoti citiem mērķiem, piemēram, lai kontrolētu darba veikšanas kvalitāti vai kvantitāti.

Kādi noteikumi jāievēro, uzstādot videonovērošanas ierīces?

Pirms videonovērošanas iekārtu uzstādīšanas darba devējam ir jāizvērtē:

- plānotie ieguvumi, uzstādot minētās ierīces un vai šie ieguvumi ir būtiskāki nekā negatīvais efekts uz darbiniekiem;
- vai ir skaidri noteikts plānotais videonovērošanas mērķis un tas ir pietiekami izskaidrots;
- vai videonovērošanas ierīču izmantošana tiešām ir nepieciešamaun un vai ir efektīvi mērķa sasniegšanai izmantot videonovērošanas ierīces;
- vai nepastāv citi efektīvi līdzekļi vai veidi, lai sasniegtu paredzēto mērķi, neizmantojot videonovērošanas ierīces (t.i., izmantojot labākas kvalitātes durvis, īpaši aizsargātus stiklus, dažādas slēdzeņu sistēmas un kustības detektorus vai citus sensorus īpašuma aizsardzībai, utt.);
- vai nepieciešams saglabāt ierakstus no videonovērošanas iekārtām, vai veikt videonovērošanu reālā laika režīmā;
- vai veikt ierakstus patstāvīgi vai tikai, ja iestājas kāds noteikts kritērijs;
- vai ir iespējams, lai sasniegtu mērķi, veikt tikai noteiktas telpas daļas novērošanu;
- vai uzstādīt mobilu videonovērošanas ierīci vai patstāvīgi filmējošu;

3 Papildus informācijai – skatīt Datu valsts inspekcijas rekomendāciju „Datu apstrāde videonovērošanas jomā"(http://www.dvi.gov.lv/lv/jaunumi/publikacijas/), kā arī Direktīvas 95/46/EK 29. panta darba grupas izstrādātos dokumentus, kas attiecas uz personas datu apstrādi darba tiesisko attiecību ietvaros (Direktīvas 95/46/EK 29. panta darba grupas pieņemtos dokumentus skatīt – http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm).

- vai videonovērošanas ierīces filmēšanas perimetrs būs nemainīgs, vai tas automātiski mainīsies vai to varēs mainīt manuāli;

- vai attēlu varēs palielināt, cik liela būs optikas izšķirtspēja, kas darīs iespējamu saskatīt sīkākās attēla detaļas, vai arī tiks iegūts daudz vispārīgāks attēls.

Videonovērošanas ierīces var tikt uzstādītas pie ēku ieejām un izejām, drošības izejām un personu pārvietošanās ceļiem. To videonovērošanas leņķis var aptvert teritorijas, jeb zonas, kur tiek glabātas preces vai citas vērtības. Tās nevar aptvert darbinieku darba vietas, izņemot atsevišķus gadījumus (piemēram, darbinieka darbs saistīts ar finanšu līdzekļiem, bet tad videonovērošanas ierīcei ir jāfilmē kasiera darbs ar finanšu līdzekļiem vai darbs noliktavā, kurā tiek glabātas vērtības un tiek attiecīgi filmēta to pārvietošana). Videonovērošana ir jāveic, ievērojot samērīgumu. Ierīces nevar tikt uzstādītas, tikai atsaucoties uz vispārēju argumentu par iespējamiem apdraudējumiem personu dzīvībai, veselībai vai īpašuma aizsardzībai.

Darba vietās darba devējam ir jārespektē darbinieka privātā dzīve. Videonovērošanas ierīces nevar tikt uzstādītas un nevar filmēt darbiniekus tādās telpās, kas domātas darbinieku atpūtai, ģērbtuvēs, tualetēs un dušas telpās. Tāpat videovērošanas ierīces nevar tikt izvietotas privātajos darba kabinetos, kā arī telpās, kas saistītas ar sensitīvu personas datu apstrādi, t.i. reliģiskajās lūgšanu telpās, arodbiedrību telpās, veselības aprūpes darbinieku telpās un pie ieejas tajās.

Aizliegts ierīces izvietot bez darbinieku informēšanas, kā arī izmantot slēptās miniatūrās kameras, ja vien normatīvie akti tieši nepieļauj to izmantošanu.

Kopumā uzskatām, ka nav tiesiski uzstādīt videonovērošanas ierīces ar skaņu ierakstu, ja vien normatīvie akti tieši nepieļauj to izmantošanu, kā arī uzstādīt videonovērošanas ierīces tikai tāpēc, ka to izmaksas ir salīdzinoši nelielas.

Kas var piekļūt videonovērošanas kameru ierakstiem?

Tikai attiecīgi pilnvarotas personas, veicot savas funkcijas, var skatīties, jeb piekļūt videonovērošanas ierakstiem (piemēram, apsardzes struktūras vadītājs). Darba devējam jāizvērtē, vai minēto pilnvaroto personu tiesības piekļūt videonovērošanas kameru ierakstiem ir skaidri noteiktas. Piemēram, vai apsardzes darbiniekam, kura pienākumos ietilpst piekļūt videonovērošanas ierakstiem, kas tiek veikti reālājā laika režīmā, vienlaicīgi ir tiesības izgatavot ierakstu kopijas. Šīm personām ir jābūt speciāli apmācītām un jāpārzin videonovērošanas sistēmas ieviešanas un uzturēšanas noteikumi. Katram pārzinim ir jāizvērtē, kad un kādu informāciju sniegt trešajām personām un vai tam pastāv likumam atbilstošs pamats un mērķis (piemēram, pēc tiesībsargājošo institūciju pieprasījuma, kurā norādīts konkrēts informācijas pieprasīšanas pamatojums).

Cik ilgi var uzglabāt videoierakstus?

Videonovērošanas kameru ieraksti jāsaglabā pēc iespējas īsāku laiku. Ieteicams tos saglabāt tikai dažas dienas, pirms tam veicot nepieciešamās incidenta pārbaudes un izmanto ierakstus, lai iniciētu disciplinārlietas, administratīvā pārkāpuma lietas vai kriminālprocesu.

Ja šādi procesi saistībā ar konstatētajiem incidentiem ir ierosināti, ieraksti var tikt izņemti no ierīces (fiksējot, ka ieraksti ir izņemti) un saglabāti tik ilgi, cik nepieciešams attiecīgajam procesam. Ja tehniski tas ir iespējams, maksimālais attēla ierakstu saglabāšanas laiks var tikt noteikts automātiski pašā sistēmā. Ierakstu glabāšanas termiņu nevar noteikt, tikai pamatojoties tikai uz tehniskās ierīces glabāšanas iespējām.

Kāda informācija jāizvieto par videonovērošanas veikšanu?

Cilvēki, kas tiek filmēti (darbinieki un apmeklētāji, klienti, u.c.), ir jāinformē par to skaidrā, nepārprotamā un saprotamā veidā, izvietojot vietās, kur notiek videonovērošana, attiecīgas zīmes, kas ietver informāciju:

- par videonovērošanas ierīces esamību;
- pārziņa (atbildīgās personas) nosaukums vai vārds, uzvārds, kā arī adrese un cita kontaktinformācija. Ja ir, tad arī personas datu operatora nosaukums, kā arī tā adrese un cita kontaktinformācija;
- paredzētais videonovērošanas mērķis un pamatojums.

Sniedzot informāciju par videonovērošanu, ir jānodrošina, lai personām būtu skaidrs, kurās vietās videonovērošana tieši tiek veikta, kā arī šīs norādes

nevar atrasties tālu no videonovērošanas veikšanas vietas jeb filmētās teritorijas.

Papildus ir ieteicams katru darbinieku informēt individuāli (piemēram, darba līguma pielikumā, darba kārtības noteikumos), tai skaitā norādot, ka darbiniekam ir tiesības piekļūt saviem personas datiem videonovērošanas sistēmas ietvaros.

VII. Pieejas kontrole darba vietām

Ņemot vērā, ka darba vietas pārsvarā gadījumu nav publiski pieejamas un to, ka darba devējiem ir nepieciešams zināt un kontrolēt darbinieka darba laiku, pieejas kontrole darba vietām jau pastāv sen. Tehnoloģiju attīstība, ieskaitot biometrijas ierīču attīstību, atvieglo šo kontroli, bet vienlaicīgi informāciju tehnoloģijas piedāvā iespēju savākt/apstrādāt vairāk informācijas par personām, tādā veidā ierobežojot personu privātumu. Tehnoloģiju izmantošanas ierobežošana ir būtiska, lai aizsargātu personu tiesības un brīvības, tai skaitā uz personas datu aizsardzību.

Kādiem mērķiem?

Darba devējs var ieviest šādas ierīces, ieskaitot biometriskās:

- pie ieejas ēkās;
- telpās, kur ir noteikts ierobežots piekļūšanas režīms.

Šo ierīču izmantošana var attiekties gan uz darbiniekiem, gan uz apmeklētājiem. Biometriskās ierīces nedrīkst tikt izmantotas, lai uzraudzītu darba laika ievērošanu un darbinieku atrašanos darba vietās, jo tas ir nesamērīgi.

Sistēma, kas ir ieviesta, lai kontrolētu darbinieku piekļūšanu darba vietām, nevar tikt izmantota citiem mērķiem, piemēram, lai kontrolētu darbinieku pārvietošanos, ierašanās un promiešanas laiku.

Kas var piekļūt datiem?

Informācija var būt pieejama tikai attiecīgi pilnvarotām personām, piemēram, iekšējo drošības dienestu darbiniekiem. Darba devējam ir jānodrošina šīs informācijas drošība un nedrīkst pieļaut nepilnvarotu personu piekļūšanu šai informācijai. To var panākt ar speciālām atļaujām, jeb pilnvarojumu piekļuvei datoriem, kā arī ieviešot obligātus attiecīgus auditācijas pierakstus, lai tie uzskaitītu visas darbības, kas tiek veiktas ar informāciju, tai skaitā, skatīšanās režīmā (t.i., kas, kad un kādiem mērķiem piekļūst informācijai).

Kāds ir datu uzglabāšanas ilgums?

Dati par pieeju darba vietām jāsaglabā pēc iespējas īsāku laiku. Rekomendējam tos dzēst pēc trim mēnešiem kopš to reģistrācijas jeb izveides.

Informācija, kas jāsniedz darbiniekiem

Darbiniekiem jābūt informētiem par personas datu apstrādes mērķiem un pamatojumu.

Rekomendējam, lai nodrošinātu personas datu godprātīgu apstrādi, informēt darbiniekus arī par:

- iespējamiem personas datu saņēmējiem;

- tiesībām izmantot savas tiesības, ko nosaka likums, tādas kā pieejas tiesības saviem datiem un tiesības izdarīt labojumus savos datos.

Darbinieka informēšanai ir jābūt noformētai skaidri, nepārprotami un saprotami. Rekomendējam, ka tā tiktu noformēta kā atsevišķs dokuments, nevis tiktu iekļauts vai pievienots pie vispārējiem noteikumiem organizācijā vai uzņēmumā.

VIII. Tālruņa izmantošana darba vietās

Tālruņu izmantošana darba vietās ir pieļaujama arī darbiniekiem personiskajiem mērķiem. Un tādējādi darba devējam, kontrolējot tālruņu izmantošanu, ir jārespektē privātuma ievērošana, t.i. vienmēr jāatceras nodrošināt, lai darbinieku novērošana un uzraudzīšana nebūtu pārmērīga, jo arī darba vietās darbinieki var sagaidīt privātuma ievērošanu noteiktā apjomā.

Vienlaicīgi darba devējam ir jāizvērtē mērķi, kādēļ tiek ieviesta sarunu ierakstīšana un vai šo mērķi nav iespējams sasniegt, īstenojot citus pasākumus vai apstrādājot personas datus mazākā apjomā. Piemēram, sarunu ierakstīšana jaunu darbinieku apmācības vajadzībām nevar notikt ilgstošā periodā vai pastāvīgi.

Kāds ir datu uzglabāšanas ilgums?

Informācija, kas tiek iegūta sarunu ierakstīšanas rezultātā, jāsaglabā pēc iespējas īsāku laiks.

Informācija, kas jāsniedz darbiniekiem

Darbiniekiem jābūt informētiem par personas datu apstrādes mērķiem un pamatojumu.

Lai nodrošinātu personas datu godprātīgu apstrādi, rekomendējam informēt darbiniekus arī par:

- iespējamiem personas datu saņēmējiem;

- tiesībām izmantot savas tiesības, ko nosaka likums, tādas kā pieejas tiesības saviem datiem un tiesības izdarīt labojumus tajos.

Darbinieka informēšanai ir jābūt noformētai skaidri, nepārprotami un saprotami. Iesakām to noformēt kā atsevišķu dokumentu, nevis iekļaut vai pievienot vispārējiem noteikumiem organizācijā vai uzņēmumā.

IX. Autotransporta aprīkošana ar ģeolokācijas sistēmām

Ņemot vērā, ka šādas ierīces kļūst lētākas un var būt ļoti noderīgas, ģeolokācijas ierīču izmantošana kļūst aizvien populārāka darba vietās un darba tiesisko attiecību ietvaros. Tomēr ir jāievēro vairāki noteikumi, izmantojot šīs ierīces, lai tiktu nodrošināts darbinieku privātums.

Kādiem mērķiem?

Ģeolokācijas ierīces var tikt izmantotas darba devēja autotransporta līdzekļos, ko izmanto darbinieki:

- lai uzraudzītu transporta pakalpojumu sniegšanu, preču piegādes un pakalpojumus, kas saistīti ar transporta līdzekli. Piemēram, ātrās palīdzības transporta līdzekļi, lai uzraudzītu sniegtos medicīnas pakalpojumus;

- lai nodrošinātu darbinieku, preču piegādes un transporta līdzekļu drošību, par ko tie ir atbildīgi;

- lai labāk izmantotu organizācijas un uzņēmuma resursus, sniedzot pakalpojumus dažādās ģeogrāfiskās vietās, ieskaitot ārkārtas gadījumus. Piemēram, lai identificētu darbinieku, kurš ir vistuvāk lifta bojājuma gadījumā vai attiecīgo medicīnisko personālu, kas ir vistuvāk nelaimes gadījumam;

- izņēmuma gadījumos, lai sekotu līdzi darba laikam, ja to nevar izdarīt savādāk;

- lai izpildītu likumā noteiktus pienākumu ieviest ģeolokācijas ierīces, ja tas saistīts ar noteiktu transporta veidu vai noteiktu preču veidu.

Izmantošanas ierobežojumi

Ierīces, kas uzstādītas darbinieku lietotajos transporta līdzekļos, nevar tikt izmantotas:

- lai uzraudzītu atbilstību ātruma ierobežojumiem; lai patstāvīgi kontrolētu darbinieku;

- ģeolokācijas ierīces nevar tikt izmantotas darbinieka transporta līdzekļos:

  - saistībā ar tā brīvību organizēt pārvietošanos,
  - lai kontrolētu darbinieku pārstāvju vai arodbiedrības pārstāvju pārvietošanos,
  - ārpus darba laika, kad darbinieks transporta līdzekli ir tiesīgs izmantot personiskām vajadzībām,
  - uzskaitīt darbinieka darba laiku, ja tam tiek izmantotas citas ierīces.

Kādas ir privātās dzīves garantijas?

Darbinieku tiesības

Darbinieks ir jāinformē par to, ka šāda ierīce ir uzstādīta. Darbiniekam ir tiesības piekļūt informācijai, kas glabājas ierīcē (pārvietošanās datums un laiks, maršruts, utt.) saskaņā ar Fizisko personu datu aizsardzības likuma 15. pantu.

Datu saņēmēji

Pieeja informācijai var būt tikai darba devējam un darbiniekiem, kas saistīti ar noteikto pakalpojumu sniegšanu.

Drošība

Lai izslēgtu nepilnvarotu personu piekļūšanu ierīcē esošajai informācijai, ir obligāti jānodrošina tās drošība. Piemēram, pieeja šai ierīcei reālajā laikā, izmantojot internetu (mājas lapu), tikai ar attiecīgu lietotājvārdu un paroli.

Datu glabāšanas laiks

Kopumā informācija, kas iegūta no ģeolokācijas ierīces, jāsaglabā pēc iespējas īsāku laiku. Rekomendējam tos dzēst pēc trim mēnešiem kopš tās reģistrācijas jeb izveides. Tomēr informācija var tikt uzglabāta ilgāk, ja tā tiek izmantota, lai optimizētu pārvietošanās maršrutus.

Darbiniekiem sniedzamā informācija

Katrs darbinieks ir jāinformē par mērķiem, kādus plānots sasniegt.

Lai nodrošinātu personas datu godprātīgu apstrādi, iesakām informēt darbiniekus arī par:

- iespējamiem personas datu saņēmējiem;
- tiesībām izmantot savas tiesības, ko nosaka likums, tādas kā pieejas tiesības saviem datiem un tiesības izdarīt labojumus tajos.

Darbinieka informēšanai ir jābūt noformētai skaidri, nepārprotami un saprotami. Iesakām to noformēt kā atsevišķu dokumentu, nevis iekļaut vai pievienot vispārējiem noteikumiem organizācijā vai uzņēmumā.

X. Citi pienākumi

Personas datu apstrādes reģistrācija Datu valsts inspekcijā

Darba devējam jāizvērtē vai nav nepieciešams reģistrēt veikto personas datu apstrādi Datu valsts inspekcijā. Papildus informāciju par personas datu reģistrāciju Datu valsts inspekcijā var iegūt Datu valsts inspekcijas sagatavotajās Vadlīnijās personas datu apstrādes reģistrācijai Datu valsts inspekcijā (skatīt - http://www.dvi.gov.lv/lv/personas-datu-apstrades-un-specialistu-registracijas-kartiba/).

Pretendenta un darbinieka tiesības piekļūt saviem datiem

Pēc pieprasījuma datu subjekts (piemēram, pretendents, darbinieks vai klients) var iegūt visu Fizisko personu datu aizsardzības likuma 15. pantā noteikto

informāciju par sevi, ko apstrādā darba devējs. Katram darbiniekam ir tiesības, apliecinot savu identitāti, iegūt visu informāciju, ko par viņu ir savācis un glabā darba devējs jeb orgnaizācija vai uzņēmums. Pārzinim šī informācija rakstveidā ir jāsniedz mēneša laikā.

Darbinieks var iegūt jebkādu informāciju, kas ir saglabāta elektroniski vai manuāli, piemēram, informāciju par karjeras vēsturi, par darba attiecību izbeigšanu, informāciju, kas saistīta ar darbinieka novērtēšanu, informāciju par disciplinārsodiem, par trešajām personām, kuras noteiktā laika posmā ir saņēmušas informāciju par darbinieku, disciplinārlietas materiāliem, utt.

Rekomendējam izstrādāt dokumentu, kas nosaka datu subjektu (t.i. pretendentu, darbinieku, klientu, u.c.) tiesības piekļūt saviem datiem, un publisko to vai savādāk darīt to zināmu datu subjektiem.

Datu subjekta tiesības labot datus

Fizisko personu datu aizsardzības likuma 16. pants nosaka, ka datu subjektam ir tiesības pieprasīt, lai viņa personas datus papildina vai izlabo, kā arī pārtrauc to apstrādi vai iznīcina tos, ja personas dati ir nepilnīgi, novecojuši, nepatiesi, pretlikumīgi apstrādāti vai arī tie vairs nav nepieciešami vākšanas mērķim. Ja persona pamato, ka tās dati ir nepilnīgi, novecojuši, nepatiesi, pretlikumīgi apstrādāti, nav nepieciešami, lai sasniegtu mērķi, kam dati tika ievākti, tad darba devējam (pārzinim) ir pienākums tos labot, un vienlaicīgi par to paziņot personām, kas iepriekš šos kļūdainos datu sir saņēmušas.

Papildus informāciju par darba tiesisko attiecību regulējumu skatīt Valsts darba inspekciajs interneta mājas lapā - *www.dvi.gov.lv*

Savukārt, saskaņā ar Darba likuma 30. pantu, individuāli tiesību strīdi starp darbinieku un darba devēju, ja tie nav izšķirti uzņēmumā, izšķirami tiesā.

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