Datu valsts inspekcija

PERSONAS DATU AIZSARDZĪBAS PĀRKĀPUMU PĀRVALDĪBA

VADLĪNIJAS

2026

Terminoloģija/saīsinājumi

Personas datu aizsardzības pārkāpums (PDAP) - ir drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.

Kiberincidents - notikums, kas apdraud apstrādātus datus vai tādu pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus piedāvā tīklu un informācijas sistēmas vai kuri pieejami ar tīklu un informācijas sistēmu starpniecību.

! Ņemot vērā, ka šo vadlīniju kontekstā PDAP būs arī kiberincidents, tad vadlīniju tekstā šie termini lietoti pamīšus, paturot prātā, ka atsevišķas vadlīnijās aprakstītās darbības būs veicamas ne tikai PDAP, bet kiberincidentam kopumā.

Incidentu reģistrs - dokuments, kurā tiek uzskaitīti notikušie kiberincidenti - gan tie, kas skar personas datus, gan tie, kas neskar.

Datu regula – Eiropas Parlamenta un Padomes 2016.gada 27.aprīļa Regula Nr.2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula).

Saturs

Ievads

Šo vadlīniju nolūks ir sniegt praktisku atbalstu organizācijas darbiniekiem un datu aizsardzības speciālistiem efektīvai un strukturētai personas datu aizsardzības pārkāpumu (turpmāk – PDAP) pārvaldībai. Vadlīnijas ir izstrādātas kā universāls rīks, lai palīdzētu atpazīt pārkāpumu, novērtēt tā riskus, fiksēt nepieciešamo informāciju un nodrošināt savlaicīgu ziņošanu uzraudzības iestādei un skartajām personām.

Lai gan vadlīniju metodoloģiskais pamats ir pārņemts no kiberincidentu pārvaldības prakses, tās ir piemērojamas jebkura veida PDAP novēršanā un izmeklēšanā – neatkarīgi no tā, vai pārkāpums noticis digitālajā vidē vai papīra formātā.

I. Kiberincidenta un personas datu aizsardzības pārkāpuma mijiedarbība

Praksē robeža starp kiberincidentu (IT drošības incidentu) un datu aizsardzības pārkāpumu bieži vien pārklājas, tomēr tie nav identiski jēdzieni. Lai nodrošinātu pareizu reaģēšanu, ir būtiski izprast to savstarpējo saiti un atšķirības:

- **kiberincidents** ir jebkurš notikums, kas apdraud informācijas sistēmu vai datu drošību (konfidencialitāti, integritāti vai pieejamību) – piemēram, *ransomware* uzbrukums, sistēmas dīkstāve vai vīruss. Kiberincidents kļūst par PDAP **tikai tad**, ja tā rezultātā ir tikuši ietekmēti (*tiem kāds ir piekļuvis, tie ir pazaudēti, izmainīti vai dzēsti*) tieši *personas dati*.
- **PDAP bez kiberkomponenta** ir pārkāpumi, kuros nav iesaistīti tehnoloģiski uzbrukumi – piemēram, dokumentu mapes pazaudēšana sabiedriskajā transportā, vēstules nosūtīšana nepareizam adresātam vai neiznīcinātu izdruku izmešana publiskā tvertnē.

Tā kā abu šo incidentu veidu pārvaldība (atklāšana, seku ierobežošana, cēloņu analīze un mācību gūšana) seko vienam un tam pašam loģiskajam ciklam, kiberincidentu izmeklēšanas struktūra ir efektīvi piemērojama arī analogu (netehnisku) pārkāpumu risināšanai.

Mijiedarbības scenāriji praksē izpaužas divējādi:

1) **Integrētā izmeklēšana (ja noticis kiberincidents ar datu noplūdi).** Ja organizācijā fiksēts kiberincidents, kura procesā skarti personas dati, PDAP izmeklēšana organiski iekļaujas kopējā kiberincidenta novēršanas gaitā. Kamēr IT drošības komanda strādā pie tehniskā cēloņa identificēšanas, sistēmu izolēšanas un "caurumu lāpīšanas", datu aizsardzības speciālisti paralēli veic ietekmes novērtējumu uz personu tiesībām un brīvībām, fiksē kompromitēto datu apjomu un gatavo paziņojumus. Abi procesi norit paralēli kā vienota mehānisma elementi.

2) Analogā izmeklēšana (ja noticis netehnisks PDAP). Ja pārkāpums nav saistīts ar kiberincidentu (piemēram, nepareizi izsniegta papīra lieta), izmeklēšanā tiek izmantota tā pati klasiskā posmu struktūra. Atšķirība ir tā, ka tehniskā risinājuma un serveru žurnālfailu (log-failu) analīzes vietā tiek izmantotas citas izmeklēšanas metodes: iesaistīto darbinieku aptaujas, telpu piekļuves kontroles izpēte vai fizisko dokumentu aprites ceļa rekonstrukcija.

Incidentu izmeklēšanas un pārvaldības posmi

1. Identifikācija

Tiek atklāts potenciāls incidents un pamanītas pirmās novirzes no normas.

Mērķis: saprast, vai vispār ir noticis incidents.

Trauksmes signāli: SIEM (drošības informācijas un notikumu pārvaldības sistēmas) brīdinājumi, antivīrusa paziņojumi, lietotāju/klientu sūdzības, sadarbības partneru ziņojumi vai pamanītas fiziskas drošības nepilnības.
Svarīgi: nekavējoties fiksēt incidenta atklāšanas laiku, iespējamo avotu un pirmās pazīmes.
Rezultāts: tiek izveidots sākotnējais incidenta reģistrācijas ieraksts (pieteikums incidentu uzskaites sistēmā vai ieraksts žurnālā).

2. Apstiprināšana un klasifikācija

Tiek veikta incidenta pirmreizējā izpēte, lai novērtētu tā raksturu un mērogu.
Mērķis: saprast, cik situācija ir nopietna un kāda ir tās ietekme.
Galvenie jautājumi:

- Vai incidents joprojām turpinās?
- Kādas sistēmas vai infrastruktūra ir skarta?
- Vai ir skarti personas dati (vai pastāv risks to kompromitēšanai)?
- Vai tas ir lokāls vai plaša mēroga incidents?

Rezultāts:

- Incidenta klasifikācija (zems, vidējs vai augsts risks).
- Lēmums par tālāko eskalāciju – informācijas nodošanu atbildīgajām struktūrvienībām (IT drošības komandai, vadībai, datu aizsardzības speciālistam (DAS) un, ja nepieciešams, CERT.LV).

Datu aizsardzības speciālista (DAS) iesaiste: ja šajā posmā tiek konstatēts, ka incidents skar vai varētu skart personas datus, par to nekavējoties tiek informēts DAS. No šī brīža paralēli kiberincidenta novēršanai tiek uzsākta potenciālā PDAP pārvaldības procedūra (tostarp 72 stundu termiņa uzskaite ziņošanai Datu valsts inspekcijai (Inspekcija; DVI)).

3. Ierobežošana un seku mazināšana

Tiek veikti tūlītēji, operatīvi pasākumi, lai nepieļautu incidenta vēršanos plašumā.
Mērķis: apturēt kaitējuma un apdraudējuma izplatīšanos.
Tipiski pasākumi:

- Skarto ierīču vai serveru atvienošana no tīkla;
- Kompromitēto lietotāju kontu bloķēšana;
- Piekļuves akreditācijas datu (paroļu, marķieru) piespiedu maiņa;
- Fiziska piekļuves liegšana skartajām telpām vai dokumentu arhīvam.

4. Izmeklēšana un risināšana

Tiek veikta dziļā analīze, lai pilnībā neitralizētu incidenta cēloņus un noskaidrotu visas detaļas.
Mērķis: noskaidrot, kas tieši notika, un pilnībā likvidēt apdraudējumu.
Kiberdrošības komanda analizē: žurnālfailus (log-failus), tīkla plūsmu, sistēmu izmaiņas un ļaunatūras paraugus.
DAS un incidenta vadītājs noskaidro un novērtē:

- Kā apdraudējums radās un kāda bija piekļuves vēsture?
- Kādi personas datu veidi ir skarti (piemēram, vispārīgie dati, finanšu dati, īpašu kategoriju dati)?
- Cik datu subjektu (personu) ir skarti?
- Kāds ir iespējamais kaitējums personām (reputācijas risks, krāpniecības risks, tiesību ierobežojumi)?

Rezultāts: tiek pieņemts galīgais, pamatotais lēmums par to, vai par notikušo PDAP ir jāziņo Datu valsts inspekcijai un vai ir jāinformē skartās personas.

5. Atjaunošana

Organizācijas darbība tiek atjaunota normālā režīmā.

Mērķis: atjaunot sistēmu un pakalpojumu drošu darbību stāvoklī, kāds tas bija pirms incidenta.
Pasākumi: ievainojamību novēršana un "lāpīšana", sistēmu atjaunošana no drošām (pārbaudītām) rezerves kopijām, piekļuves kontroles tiesību pārskatīšana un pastiprināta sistēmu uzraudzība pēc darbības atsākšanas.

6. Mācības un secinājumi (pēc-incidenta analīze)

Procesa izvērtēšana pēc tam, kad krīze ir pārvarēta.

Mērķis: izdarīt secinājumus un veikt korekcijas organizācijas procedūrās, lai mazinātu līdzīgu incidentu atkārtošanās risku nākotnē.

Pasākumi:

- kopīga izmeklēšanas ziņojuma sagatavošana (apvienojot IT tehniskos secinājumus un DAS juridisko vērtējumu);
- kļūdu identificēšana (kas nenostrādāja procesos, tehnoloģijās vai darbinieku rīcībā);
- drošības politiku, iekšējo procedūru un tehnisko kontroles pasākumu atjauninašana;
- ja nepieciešams – papildu apmācību organizēšana darbiniekiem.

! Svarīga norāde vadlīniju lietotājiem. Šajā nodaļā aprakstītie seši secīgie posmi parāda, ka PDAP izmeklēšanai nepieciešamā informācija (skartie dati, apjoms, laiks, ietekme) tiek iegūta tieši kiberincidenta pārvaldības procesā.

Lai nodrošinātu šo vadlīniju efektīvu izpildi, ieteicams noskaidrot un saskaņot rīcību ar savas organizācijas IT drošības struktūrvienību vai ārpakalpojuma sniedzējiem. Izprotot viņu ieviesto incidentu izmeklēšanas metodiku, būs skaidrs, kurā brīdī un no kādiem avotiem ir iegūstama informācija, kas nepieciešama šo vadlīniju 2.– 4. solī, lai pilnvērtīgi sagatavotu un iesniegtu paziņojumu par notikušu datu aizsardzības pārkāpumu.

Kiberincidentu izmeklēšanai un ziņošanai par tiem vērtīgs palīgresurss ir arī Nacionālā Kiberdrošības centra izstrādātās vadlīnijas "Kiberincidentu ziņošanas vadlīnijas".

II. Tehniskie un organizatoriskie pasākumi datu (ne tikai personas datu) drošībai

Lai organizācija spētu efektīvi identificēt un pārvaldīt incidentus, ir jāpārzina esošais drošības brieduma līmenis. Šis pārskats kalpo kā organizācijas "mājasdarbs" un pamats, uz kura tiek būvēta visa praktiskā incidentu novēršana.

Zemāk minētais pasākumu uzskaitījums ir indikatīvs un nav pilnīgs. Tehnoloģiju attīstība, organizācijas iekšējo procesu specifika un apstrādāto datu raksturs (piemēram, īpašu kategoriju dati) var pieprasīt citu, specifisku vai progresīvāku drošības risinājumu ieviešanu, kas nav minēti šajās vadlīnijās. Tomēr zemāk uzskaitītie pasākumi ir tas pamats, kas būtu ieviešams katrai organizācijai, kā arī sākotnējas darbības, kas katrai organizācijas jāpārdomā.

1. Tehniskie drošības pasākumi (infrastruktūra)

- **Piekļuves tiesību kontrole:** lietotāju profili, lomas un stingra tiesību piešķiršanas/anulēšanas kārtība.
- **Identifikācija:** paroļu politika (sarežģītība, derīguma termiņš) un obligāta vairākfaktoru autentifikācija (MFA/2FA) kritiskajos mezglos.
- **Datu aizsardzība un rezerves kopēšana:** portatīvo ierīču un serveru šifrēšana, regulāra rezerves kopiju (backup) veidošana un to atjaunošanas testēšana.
- **Monitorings:** centralizēta žurnālfailu (logs) veidošana, antivīrusu, ugunsmūru un ielaušanās atklāšanas sistēmu (IDS/IPS) uzturēšana.
- ***Citi pasākumi atkarībā no specifikas:*** datu noplūdes novēršanas (DLP) sistēmas, tīkla segmentācija, gala iekārtu noteikšanas un reaģēšanas (EDR) risinājumi u.c.

2. Organizatoriskie drošības pasākumi (procesi un to apraksti)

- **Iekšējie standarti:** datu aizsardzības politika, skaidri noteikumi par dokumentu apriti, klasifikāciju, glabāšanas termiņiem un iznīcināšanu.
- **Cilvēkfaktora risku mazināšana:** regulāras darbinieku apmācības, plānotie pikšķerēšanas (*phishing*) treniņi un konfidencialitātes saistību parakstīšana.
- **Tiesiskā drošība:** pārziņa un apstrādātāju līgumi ar atbilstošām drošības klauzulām pirms datu nodošanas trešajām pusēm.
- ***Citi pasākumi atkarībā no specifikas:*** regulārs ārpakalpojumu sniedzēju audits, fiziskās piekļuves zonas zonēšana, specifiskas amatu rotācijas politikas u.c.

Drošības pasākumu un procesu efektivitātes pārskatīšanas sistēma

Lai nodrošinātu pastāvīgu organizācijas gatavību, ieviestie tehniskie un organizatoriskie pasākumi nevar būt statiski. Organizācija nosaka principu, ka visi drošības pasākumi tiek pakļauti regulārai efektivitātes kontrolei:

1. *Plānveida izvērtēšana:* ne retāk kā reizi gadā organizācija veic preventīvu sistēmu auditu un darbinieku izglītošanas efektivitātes pārbaudi (piemēram, simulācijas).
2. *Ārpuskārtas izvērtēšana:* organizācija paredz obligātu drošības kontroles pasākumu revīziju pēc katra reāla PDAP, lai identificētu nepilnības esošajā aizsardzības sistēmā.

!Svarīga norāde vadlīniju lietotājiem. *D*rošības kontroles pasākumu izstrādē un uzturēšanā iespējams ieviest starptautiski atzītu standartu principus, jo īpaši ISO/IEC 27001 (Informācijas drošības pārvaldības sistēmās) un ISO/IEC 27002 (Informācijas drošības kontroles).

III. Personas datu aizsardzības pārkāpumu pārvaldības praktiskie soļi

Lai teorētisko incidentu izmeklēšanas struktūru ieviestu ikdienas darbā, organizācijai ir jāiziet noteikts praktisko darbību cikls. Šajā nodaļā ir detalizēti aprakstīts rīcības algoritms pa soļiem, kas aptver visu procesu – sākot no preventīviem sagatavošanās darbiem (pirms incidents ir noticis) līdz pat galīgajiem secinājumiem un procesu uzlabošanai pēc pārkāpuma novēršanas.

Efektīva PDAP pārvaldība nav iespējama bez savlaicīga mājasdarba, tāpēc pirmais solis ir vērsts uz organizācijas gatavības nodrošināšanu.

1. solis

Noteikt, kas uzskatāms par datu aizsardzības pārkāpumu, un sagatavoties tā pārvaldībai

Mērķis: nodrošināt organizācijas gatavību ātrai un precīzai rīcībai, lai savlaicīgi atpazītu un identificētu jebkuru incidentu, kas skar vai var skart personas datus.

Preventīvo pasākumu un sagatavošanās posma galvenais uzdevums ir panākt, lai brīdī, kad notiek incidents, organizācijā valdītu skaidrība, nevis haoss. Darba izpilde PDAP pārvaldībā sākas vēl pirms paša pārkāpuma, sakārtojot iekšējos procesus, kritērijus un metodikas.

1.1. Personas datu aizsardzības pārkāpuma klasifikācija

Sasniedzamais rezultāts

Organizācijā ir ieviesta vienota, dokumentēta PDAPklasifikācijas sistēma. Ir noteikti skaidri incidentu kvalificēšanas kritēriji, identificēti iespējamie pārkāpumu veidi ikdienas procesos un izstrādāts pārkāpumu katalogs, kas ļauj nekavējoties noteikt sākotnējo riska līmeni un ietekmi uz fizisko personu tiesībām un brīvībām.

Veicamie pasākumi

Lai incidentu izmeklēšana būtu konsekventa, organizācijai jāizstrādā vienota pārkāpumu klasifikācijas un izmeklēšanas sistēma. Šīs sistēmas pamatā ir trīs secīgi un savstarpēji saistīti pasākumi, kas nodrošina vienotu izpratni organizācijas ietvaros.

1. Kvalifikācijas kritēriju noteikšana

Organizācijai ir skaidri jādefinē un jādokumentē kritēriji, pēc kuriem konkrēts drošības notikums organizācijā tiek kvalificēts kā PDAP. Par PDAP ir uzskatāms tikai tāds incidents, kas neatkarīgi no nodoma vai tehniskā cēloņa izraisa nejaušu vai nelikumīgu organizācijas apstrādē esošo personas datu iznīcināšanu, nozaudēšanu, pārveidošanu, neautorizētu izpaušanu vai piekļuvi tiem. Ja incidents neietekmē fizisko personu datus (piemēram, mājaslapas dīkstāve bez datu apstrādes funkcionalitātes), tas tiek risināts standarta IKT drošības procedūru ietvaros.

2. Procesu risku apzināšana un ietekmes novērtēšana

Organizācijai ir jāidentificē un jāapzina iespējamie PDAP veidi organizācijas ikdienas procesos (piemēram, datu noplūde, neatgriezenisks datu zudums, autorizācijas tiesību pārkāpumi u.c.). Izvērtējot šos procesus, tiek novērtēta potenciālā ietekme un iespējamais kaitējums fizisko personu tiesībām un brīvībām, piemēram, finanšu zaudējumi, identitātes zādzība, diskriminācija vai kaitējums reputācijai.

3. Klasifikācijas apraksta izveide ar praktiskiem piemēriem

Praktiski tas nozīmē, ka vispirms rakstiski tiek definēti PDAP veidi (konfidencialitātes, integritātes un pieejamības pārkāpumi) un katram no tiem tiek pievienoti tipiski piemēri no organizācijas darbības, norādot potenciālās ietekmes uz skartajām personām un sākotnējo riska līmeni (zems/vidējs/augsts):

- **Konfidencialitātes pārkāpums** - situācija, kad, piemēram, e-pasts ar klienta veselības vai citiem personas datiem tiek nosūtīts nepareizam adresātam, nepiederošs darbinieks piekļūst cilvēkresursu sistēmai vai kļūdaini publiski tiek padarīts pieejams fails ar klientu datiem u.c.
    - *Sākotnējais risks:* parasti vidējs līdz augsts (atkarībā no skarto datu veida un pieejamības loka).
- **Integritātes pārkāpums** - rodas, ja, piemēram, sistēmas kļūdas dēļ klientiem tiek piešķirta nepareiza adrese vai darbinieks apzināti pamaina klienta konta datus u.tml.
    - *Sākotnējais risks:* vidējs (var radīt tiesiskas sekas, kļūdainus darījumus vai komunikācijas riskus).
- **Pieejamības pārkāpums** - ir situācija, ja, piemēram, rezerves kopijas nav veiktas un sistēmas kļūmes dēļ dzēsti klientu līgumi vai, piemēram, *ransomware* (izspiedējprogrammatūras) uzbrukuma rezultātā dati vairs nav pieejami (arī, ja tas notiek uz īsu brīdi).
    - *Sākotnējais risks:* no zema līdz augstam (atkarībā no datu atjaunošanas ātruma un dīkstāves ietekmes uz kritisko pakalpojumu sniegšanu).

1.2. Personas datu aizsardzības pārkāpuma identificēšana

Sasniedzamais rezultāts
Organizācija spēj noteikt, ka noticis PDAP, un zina, kam un kā par to jāziņo.

Veicamie pasākumi:

- Izveidot skaidru iekšējo procedūru (ceļa karti), kā organizācijā tiek identificēti pārkāpumi, kādi uzraudzības mehānismi tiek izmantoti un kuras personas (piemēram, IT nodaļa, DAS, struktūrvienību vadītāji) ir atbildīgas par pirmreizējo pārbaudi.
- Sagatavot un padarīt darbiniekiem pieejamus vienkāršus incidentu atpazīšanas kritērijus, kas palīdz nodalīt ikdienas tehnisko kļūmi no datu aizsardzības pārkāpuma.

Praktiskie kritēriji PDAP atpazīšanai
Lai darbinieks saprastu, vai radusies situācija varētu būt PDAP, viņam jāatbild uz pieciem jautājumiem, kas izriet no datu drošības pamatprincipiem:

PDAP atpazīšanas jautājumi:

- Vai notikums saistāms ar identificētu vai identificējamu fizisku personu ?
- Vai dati varēja nonākt nepiederošu personu rīcībā?
- Vai dati tika mainīti bez atļaujas?
- Vai dati kļuva nepieejami uz laiku vai neatgriezeniski?

Piemēram, darbinieks saņem klienta e-pastu, kurā norādīts: "Man atsūtīta cita klienta rēķina kopija". E- pastam pievienoti arī attiecīgie dokumenti. Šajā situācijā darbinieks, ievērojot noteiktos kritērijus, saprot, ka:

- *tie ir personas dati (vārds, uzvārds, adrese, bankas informācija);*
- *šie dati nonākuši pie personas, kurai tie nav domāti.*

Saskaņā ar šo darbinieks nekavējoties ziņo atbilstoši iekšējai incidentu ziņošanas procedūrai.

Tehniskie un fiziskie avoti pārkāpumu identificēšanai
Lai organizācija spētu laikus pamanīt pārkāpumus (īpaši tos, par kuriem neziņo klienti), tiek izmantoti šādi datu avoti un uzraudzības mehānismi:

- **Informācijas sistēmu digitālie audiologi (žurnālfaili):** sistēmu auditācijas pierakstu analīze, brīdinājumi par neautorizētiem vai neparasti apjomīgiem datu eksportēšanas/piekļuves mēģinājumiem.
- **Fiziskās drošības kontroles dati:** telpu piekļuves karšu reģistrācijas dati, videonovērošanas ieraksti (publiski pieejamās vai ierobežotas piekļuves telpās), apsardzes ziņojumi.
- **Lietotāju tiesību audits:** regulāras pārbaudes attiecībā uz darbinieku piekļuves tiesību apjomu (vai tiesības atbilst amata aprakstam) un kontrole pār to, kuriem darbiniekiem ir piekļuve sistēmu rezerves kopijām (backups).

Piezīme. Iekšējās procedūras attiecībā uz integritātes un pieejamības risku identificēšanu ir jāpielāgo katras konkrētās organizācijas informācijas sistēmu specifikai (piemēram, datubāžu replikācijas kļūdas, monitoringa rīku brīdinājumi u.c.).

1.3. Iekšējā ziņošanas procedūra

Sasniedzamais rezultāts: organizācijā ir ieviesta un praktiski darbojas skaidra iekšējā kārtība, kas nodrošina, ka darbinieki zina, kur, kā un cik ātri jāziņo par pamanītām drošības nepilnībām vai iespējamiem datu pārkāpumiem. Procedūra ir dokumentēta, pieejama un praktiski izmantojama (ne tikai "uz papīra").

Veicamie pasākumi
Iekšējā ziņošanas procedūra ir organizācijas iekšējā kārtība, kurā skaidri aprakstīts, kā darbiniekiem jāziņo par pārkāpumiem, tai skaitā drošības incidentiem, kas skar personas datus. Tajā parasti nosaka atbildīgās personas, kurām ziņot, kā ziņot, cik ātri ir jāziņo (piemēram, 2 stundu laikā pēc tā atklāšanas un kas notiek tālāk ar šo ziņojumu, kurš izmeklē, kā tas tiek reģistrēts un kā tiek pieņemti lēmumi par attiecīgo incidentu). Tā ir rakstiska instrukcija, procedūra, kas palīdz nodrošināt, ka neviens incidents netiek "noklusēts" un visi gadījumi tiek izskatīti vienādi un savlaicīgi.

! Svarīga terminoloģijas piezīme - lai organizācijā neradītu apjukumu, vadlīnijās tiek izmantoti divi jēdzieni:

- **Drošības incidents** – jebkurš aizdomīgs notikums vai tehniska kļūme (plašāks jēdziens).
- **PDAP** – drošības incidents, kura rezultātā ir reāli skarti personas dati (šaurāks jēdziens).

Darbinieka uzdevums nav pašam noteikt, vai ir noticis PDAP. Darbinieka pienākums ir ziņot par jebkuru aizdomīgu drošības incidentu.

Izstrādājot un apstiprinot iekšējo incidentu ziņošanas kārtību, tajā obligāti jāiekļauj šādi pieci pamata elementi:

1) Ziņojumu saņemšanas kanāli un avoti

Kārtībā precīzi nosaka, no kurienes organizācija var saņemt informāciju un kādus kanālus darbiniekam jāizmanto ziņošanai par incidentu.

- **Primārie ziņošanas kanāli organizācijā:**
  - ✓ specializēta, centralizēta e-pasta adrese (piemēram, *incidenti@organizacija.lv*);
  - ✓ tieša ziņošana par datu apstrādi atbildīgajai personai/ DAS;
  - ✓ paziņojuma reģistrēšana organizācijas iekšējā IT palīdzības dienesta (Helpdesk) sistēmā.
- **Incidentu iespējamie avoti:**
  - ✓ *iekšējais avots:* darbinieks, kurš ikdienas darbā pamana aizdomīgu aktivitāti (neparasti sistēmas paziņojumi, svešas piekļuves tiesības).
  - ✓ *ārējais avots (klienti):* fizisku personu sūdzības vai iesniegumi (piemēram, saņemts svešs rēķins).
  - ✓ *sadarbības partneri:* ārpakalpojumu sniedzēji (IT uzturētāji, mākoņpakalpojumu sniedzēji), kas informē par konstatētu ievainojamību vai sistēmas uzlaušanu.
  - ✓ *trešās personas:* nejauši informācijas saņēmēji, valsts iestādes vai drošības pētnieki.

2) Ziņošanas termiņš
Kārtībā apraksta konkrētu laiku, cik ātri jāziņo, piemēram:

- darbiniekam jāziņo savam tiešajam vadītājam par iespējamu PDAP ne vēlāk kā 2 stundu laikā pēc tā atklāšanas;

- ziņojums ir jānosūta nekavējoties ar tiem faktiem, kas ir pieejami konkrētajā brīdī. Nav jāgaida pilnīga situācijas skaidrība vai detalizēta izpēte, informāciju var papildināt un precizēt vēlāk.

3) Ziņojuma minimālais saturs
Kārtībā apraksta, kāda informācija obligāti jānorāda ziņojumā, lai atbildīgie varētu ātri sākt izmeklēšanu. Ziņojumā jāiekļauj šāda minimālā informācija:

- **kas notika** - īss un skaidrs notikuma apraksts;
- **kad incidents notika vai tika atklāts** – norāda precīzu datumu un laiku;
- **kas ir skarts** - ja ir zināms, tad norāda, kādas informācijas sistēmas, lietotnes ir skartas;
- **datu apjoms -** aptuvenais skarto personu (datu subjektu) skaits un datu veidi (piemēram, personu kodi, medicīnas dati, finanšu dati);
- **veiktās darbības -** kādi tūlītējie pasākumi jau veikti, ja ir veikti (piemēram, atslēdzis datoru no tīkla);
- **ziņotājs -** norāda vārdu, uzvārdu, struktūrvienību un kontakttālruni.

Ieteicams izstrādāt standarta incidenta formu (papīra vai elektronisku), lai visi ziņojumi būtu vienotā formātā.

4) Atbildīgās personas.
Kārtībā ir skaidri jānosaka lomas, proti, kurš pieņem ziņojumu un kurš vada procesu. Šīs personas bieži vien veido organizācijas Incidentu novēršanas komandu:

- **par informācijas sistēmām atbildīgā persona (IKT drošības pārvaldnieks)** atbild par tehnisko infrastruktūru, žurnālfailu apkopošanu un kiberincidenta tehnisko ierobežošanu.
- **datu aizsardzības speciālists (DAS)** izvērtē incidenta juridisko pusi, vai tas kvalificējas kā PDAP, kādi ir riski fiziskām personām, un vai par to ir jāziņo Datu valsts inspekcijai.
- **struktūrvienības / procesa vadītājs** nodrošina biznesa procesa kontekstu un sniedz informāciju par to, kādi tieši dati un kāpēc šajā procesā tika apstrādāti.

5) Ziņojuma apstrāde, izmeklēšana un lēmumu pieņemšana
Kārtībā apraksta, kas notiek tālāk ar šo ziņojumu, kurš izmeklē, kā tiek reģistrēts un kā tiek pieņemti lēmumi par attiecīgo incidentu. Tiklīdz ziņojums ir saņemts, sākas oficiālais pārvaldības process:

- ziņojuma saņemšana un reģistrēšana, kas paredz noteiktu laika periodu, kurā atbildīgā persona reģistrē ziņojumu, piemēram, nekavējoties (ne vēlāk kā 1-2 stundu laikā no saņemšanas brīža);
- piešķir incidentam unikālu identifikācijas numuru un ieraksta incidentu Incidentu reģistrā, norādot pamatinformāciju (datums, īss apraksts, ziņotājs, skarto datu veids, iesaistītās sistēmas);
- kā tiek veikta sākotnējā pārbaude un incidenta apstiprināšana, piemēram, atbildīgā persona veic sākotnējo pārbaudi, lai apstiprinātu incidenta faktu un pieņemtu lēmumu par tā tālāko virzību (vai tas tiek virzīts kā standarta IT incidents, vai tiek iedarbināts PDAP novēršanas protokols).

1.4. Incidenta izmeklēšanas process

Kārtībā apraksta, kā tiek veikta incidenta padziļināta izmeklēšana un riska novērtējums, piemēram, kurš atbild par šo procesu un kas tiek veikts izmeklēšanas laikā. Izmeklēšanas laikā obligāti tiek noskaidroti un dokumentēti šādi fakti:

- **Datu veids:** noskaidrots precīzs skarto personas datu veids (piemēram, vispārīgie dati, finanšu dati, piekļuves paroles, īpašu kategoriju personas dati).
- **Mērogs:** noteikts skarto datu subjektu (fizisko personu) un datu ierakstu aptuvenais skaits.
- **Cēloņsakarība:** analizēts incidenta izraisīšanas cēlonis (piemēram, mērķtiecīgs ārējs kiberuzbrukums, darbinieka kļūda/cilvēkfaktors, sistēmas tehniskā kļūme vai iekšējas ļaundabīgas rīcības sekas).
- **Riska pakāpe:** veikts formāls riska novērtējums attiecībā uz fizisko personu tiesībām un brīvībām, klasificējot to trīs līmeņos (zems, vidējs vai augsts risks), piemēram, izmantojot Eiropas Kiberdrošības aģentūras (ENISA) metodiku.

.

1.5. Lēmumu pieņemšana par ziņošanu Inspekcijai un datu subjektiem

Kārtībā apraksta, kā tiek pieņemts lēmums par turpmāko rīcību:

- vai un kā ziņot par notikušo Inspekcijai, ja risks personu tiesībām ir vidējs vai augsts organizācijai ir pienākums paziņot DVI par notikušo PDAP **72 stundu** laikā kopš pārkāpuma uzzināšanas brīža;
- vai informēt skartos datu subjektus, ja riska novērtējums uzrāda **augstu risku**, organizācijai ir pienākums bez nepamatotas kavēšanās tiešā un saprotamā veidā informēt pašas skartās personas.

Galīgo lēmumu par ziņošanu/neziņošanu pieņem vadība, piemēram, organizācijas vadītājs vai cita pilnvarota persona, un šis lēmums tiek fiksēts Incidentu reģistrā un iekšējā izvērtējumā.

1.6. Pēc-incidenta izvērtējums un praktiskā sistēmas pilnveide

Kārtībā apraksta, kā organizācijā tiek organizēts un dokumentēts pēc-incidenta izvērtēšanas process pēc tam, kad incidents ir tehniski ierobežots un visi nepieciešamie paziņojumi Inspekcijai vai datu subjektiem ir nosūtīti.

Kārtībā iekļauj šādus noteikumus:

- **slēgšanas ziņojuma sagatavošanas termiņi un adresāts:** kārtībā nosaka, kādā termiņā krīzes (incidentu novēršanas) komanda pēc incidenta seku pilnīgas likvidēšanas sagatavo un iesniedz organizācijas vadībai detalizētu incidenta slēgšanas ziņojumu;
- **pamatcēloņu un drošības plaisu analīze (*"kas nenostrādāja?"*):** kārtībā paredz pienākumu veikt strukturētu analīzi, lai identificētu precīzu posmu, kurā esošie aizsardzības mehānismi ir pievīluši. Ziņojumā obligāti vērtē, vai incidents noticis nepilnīgas preventīvās drošības bāzes dēļ (piemēram, vāja paroļu politika, tehniski trūkumi sistēmās) vai arī nostrādājis cilvēkfaktors (piemēram, nepietiekama darbinieku modrība);
- **korektīvo pasākumu ieviešana un drošības bāzes aktualizācija:** kārtībā nostiprina prasību, ka, balstoties uz izvērtējuma rezultātiem, organizācijai ir pienākums ieviest reālus un izmērāmus uzlabojumus. Tas ietver tehnisko konfigurāciju maiņu, iekšējo procesu pilnveidi vai specifisku, mērķtiecīgu darbinieku apmācību organizēšanu;
- **incidentu reģistra ieraksta noslēgšana:** kārtībā nosaka, ka visi veiktie secinājumi, ieviestie korektīvie pasākumi un veiktie uzlabojumi ir oficiāli jādokumentē, izdarot attiecīgu ierakstu organizācijas incidentu reģistrā. šis ieraksts kalpo kā tiesisks un praktisks apliecinājums tam, ka organizācijas drošības bāze ir faktiski aktualizēta un pilnveidota.

Paraugs: Kiberincidenta izmeklēšanas veidlapa (skatīt pielikumā).

Iespējams izmantot arī cert.lv sagatavotās kārtības un incidentu reģistru kā paraugu.

2. solis

Personas datu aizsardzības pārkāpuma izmeklēšana

Mērķis: precīzi apzināt notikušā apstākļus, noteikt skarto datu apjomu un raksturu, kā arī novērtēt iespējamo apdraudējumu fiziskām personām, lai pieņemtu pamatotus lēmumus par seku likvidēšanu un ziņošanu.

2.1. Sākotnējā analīze un klasifikācija

Sasniedzamais rezultāts

Nekavējoties veikta incidenta pirmreizējā izpēte un fiksēti pamatfakti, lai identificētu, vai notikums ir uzskatāms par PDAP. Noteikts pārkāpuma veids (konfidencialitāte, integritāte vai pieejamība), provizoriskais mērogs un ietekmētās sistēmas, kas ļauj operatīvi uzsākt seku ierobežošanu un plānot tālākos izmeklēšanas resursus.

Veicamie pasākumi

Sākotnējā analīze ir tūlītēja reaģēšana uz saņemto ziņojumu (no darbinieka, sistēmu monitoringa rīkiem vai trešajām pusēm). Tās mērķis nav veikt pilnu, galīgo izpēti, bet gan iegūt pietiekamu informāciju par incidenta būtību, lai nekavējoties:

1) saprastu, vai incidents vispār skar personas datus (vai tas ir "tīrs" IKT drošības incidents, vai arī PDAP);
2) noteiktu incidenta prioritāti un svarīguma pakāpi;
3) pieņemtu lēmumu par nepieciešamajiem papildu resursiem un tūlītējiem seku ierobežošanas soļiem.

Par incidentu pārvaldību atbildīgā persona, neveicot laikietilpīgu padziļinātu izpēti, nekavējoties pārbauda saņemtā ziņojuma pamatfaktus un veic pirmo ierakstu organizācijas Incidentu reģistrā.

Sākotnējā ierakstā obligāti fiksē atbildes uz šādiem pamatjautājumiem:

- **Laika rāmis (kad?):** incidenta iespējamais norises datums/laiks un precīzs brīdis, kad organizācija to faktiski atklāja (no šī brīža sākas Datu regulā noteiktais 72 stundu termiņš).
- **Notikuma būtība (kas notika?)**: īss un lakonisks situācijas apraksts (piemēram, *e-pasts ar klientu datiem nosūtīts nepareizam adresātam; šifrēšanas vīrusa uzbrukums serverim*).
- **Datu raksturs (kādi dati?):** vai ir skarti personas datus un kādas kategorijas (piemēram, vārdi/uzvārdi, personas kodi, finanšu dati, piekļuves paroles vai īpašu kategoriju dati, piemēram, veselības dati).
- **Mērogs (cik personu?):** provizorisks skarto fizisko personu skaits (vai tie ir daži klienti, visi darbinieki vai visa datubāze).
- **Incidenta avots (kur?):** kādas sistēmas, programmatūra vai fiziskie procesi (piemēram, papīra dokumentu arhīvs) ir iesaistīti.
- **Pārkāpuma klasifikācija (kāds veids?)**: incidenta tipa noteikšana atbilstoši Eiropas Datu aizsardzības kolēģijas (EDAK) Pamatnostādnēm par personas datu aizsardzības pārkāpumu paziņošanu saskaņā ar Regulu (ES) 2016/679 (sīkāk aprakstīts 1.1. sadaļā):

- *konfidencialitātes pārkāpums*.
- *integritātes pārkāpums*.
- *pieejamības pārkāpums:*.

- **Sākotnējais riska izvērtējums (kādas sekas?)**: pirmšķietamais novērtējums par to, vai un cik nopietnu apdraudējumu šis notikums rada skarto fizisko personu tiesībām un brīvībām (piemēram, vai pastāv identitātes zādzības, finanšu zaudējumu vai diskriminācijas risks).

Piemēram, darbinieks ziņo atbildīgajai personai, ka ir nosūtījis klientam rēķinu, bet pielikumā kļūdas dēļ pievienojis arī cita klienta rēķinu. Sākotnējās analīzes laikā tiek konstatēts, ka incidents noticis, izmantojot Microsoft Outlook un grāmatvedības sistēmu, un rēķinā ir iekļauti šādi personas dati: cita klienta vārds, uzvārds, piegādes adrese, kontaktinformācija un rēķina summa. Tiek secināts, ka skarta viena fiziska persona (klients B) un, ka tas ir konfidencialitātes pārkāpums, jo dati atklāti nepiederošai personai (klientam A). Ņemot vērā, ka nav iesaistīti īpašās kategorijas dati, bet tomēr ir finanšu informācija, sākotnējais riska līmenis tiek vērtēts kā zems. Šī minimālā informācija tiek ierakstīta Incidentu reģistrā, un atbildīgā persona turpina incidenta padziļinātu izmeklēšanu.

2.2. Padziļinātās izmeklēšanas saturs un noskaidrojamā informācija

Sasniedzamais rezultāts

Ir veikta vispusīga un pierādījumos balstīta incidenta izpēte, atlasot un dokumentējot visu nepieciešamo tehnisko un organizatorisko informāciju. Izmeklēšanas process nodrošina vienotu un konsekventu pieeju, kas ļauj objektīvi novērtēt pārkāpuma raksturu un tā ietekmi uz datu subjektiem.

Veicamie pasākumi

Uzsākot padziļināto izpēti, par incidentu pārvaldību atbildīgā persona kā sākotnējo filtru izmanto 1.1. apakšnodaļā noteikto klasifikāciju. Katrs incidents tiek piesaistīts vienam vai vairākiem pārkāpuma veidiem (konfidencialitāte, integritāte vai pieejamība), kas noteic tālāko izmeklēšanas fokusu un tehnisko metožu izvēli.

Lai netiktu izlaists neviens būtisks aspekts un organizācija spētu sniegt izsekojamu pamatojumu saviem lēmumiem, informācijas apkopošana tiek veikta divos secīgos līmeņos - no vispārīgā uz specifisko.

I. LĪMENIS: Pamata informācijas kopa (jāapkopo visos gadījumos)

Neatkarīgi no incidenta veida vai tehniskās sarežģītības, izmeklēšanas sākumposmā obligāti ir jānoskaidro un jāfiksē šāda pamata informācijas kopa, kas ļauj novērtēt incidenta ietekmi:

1. Skarto datu subjektu kategorijas:

Jāidentificē pārkāpuma skartās fizisko personu grupas. Izmantojot organizācijas Datu apstrāžu reģistru un sistēmu aprakstus, tiek noskaidrots, vai incidents attiecināms uz klientiem (un vai uz visiem), vai tas skāris darbiniekus un kādā apjomā. Incidenta tehniskais apkopojums ļauj saprast, kuras sistēmas ir skartas, savukārt šajā solī tiek precizēts, kuru personu tiesības ir apdraudētas.

2. Iesaistīto personas datu kategorijas:

Tiek secināts, kādi tieši dati ir kompromitēti. Izmantotās informācijas sistēmas lielākajā daļā gadījumu ļauj šo soli veikt reizē ar skarto datu subjektu kategoriju apkopošanu. Piemēram, secinājums, ka skarta organizācijas personālvadības sistēma, ļauj tieši secināt, ka skartas tādas personas datu kategorijas kā personas kodi, finanšu dati, algas vai darba līgumu saturs.

3. Faktiskais apjoms un cēlonis:

- *Apjoms:* jānosaka precīzs vai maksimāli tuvs aptuvenais skarto personu (datu subjektu) skaits un kompromitēto datu lauku apjoms.

- *Cēlonis:* jānosaka precīzs ierosināšanas notikums (cilvēkfaktors, sistēmas darbības kļūda vai mērķtiecīgs ārējs uzbrukums). Ja cēlonis ir cilvēciska kļūda (piemēram, sajauktas e-pasta adreses), apjoma vērtējums ir tūlītējs un precīzs, ja tas ir ārējs uzbrukums, jānosaka visi skartie sistēmas elementi un tajos esošie dati.

4. Datu tehniskais statuss un konteksts: jāiegūst informācija par pašu datu stāvokli pārkāpuma brīdī. Ja datu masīvi sistēmā atrodas šifrēti vai pseidonimizēti un šifrēšanas atslēgas nav zaudētas, riski datu subjektiem ir būtiski mazāki. Tāpat jāvērtē datu konteksts - dati, kas satur tikai daļu no kopējās informācijas (piemēram, adresi bez piesaistīta vārda vai identifikatora), rada mazāku ietekmes risku nekā pilna datu subjekta profila zudums.

5. Precīza notikumu secība (hronoloģija): jāfiksē precīza laika līnija no pārkāpuma faktiskā sākuma brīža, atklāšanas brīža līdz pilnīgai seku lokalizēšanai.

! Jāpatur prātā, ka šī informācija izmeklēšanas sākumā nav statiska. Izmeklēšanas gaitā ziņas var mainīties - var atklāties jaunas datu kopas vai, tieši otrādi, noskaidroties, ka incidents ir mazāks, nekā šķita sākotnēji. Apkopotā informācija ir jāuztver kā dinamiska platforma, kas tiek papildināta visā procesa gaitā.

II. LĪMENIS: Specifiski noskaidrojamā informācija (pielāgo pēc pārkāpuma rakstura)

Pēc vispārīgo faktu noskaidrošanas izmeklēšana tiek virzīta dziļumā, veicot specifiskas darbības un iegūstot datus atbilstoši incidenta klasifikācijai.

1) Informācijas iegūšana konfidencialitātes pārkāpumu gadījumos

Ja konstatēts konfidencialitātes pārkāpums, galvenais fokuss ir noskaidrot, kam tieši personas dati ir tapuši pieejami, un veikt pasākumus, lai mazinātu šī incidenta radīto kaitējumu. Izmeklēšanas gaitā tiek veiktas šādas darbības:

- **piekļuves un saņēmēju identificēšana:** tiek pārbaudīti e-pasta žurnālfaili (logi), piekļuves tiesības sistēmās, mājaslapas vai citu resursu piekļuves statistika, lai precīzi fiksēju, kurš ir atvēris vai lejupielādējis attiecīgo failu vai saņēmis sūtījumu.
- **datu rakstura un apjoma izvērtēšana:** tiek noteikts, kāda veida informācija trešajām personām bijusi redzama (piemēram, tikai ierobežota kontaktinformācija, vai arī pilns personas kods, finanšu dati, īpašu kategoriju/veselības dati), kā arī precīzs skarto datu subjektu skaits.
- **datu nodošanas riska pārbaude:** tiek noskaidrots, vai dati nav saglabāti, pārsūtīti tālāk vai citādi reproducēti (piemēram, vai e-pastam nav bijuši papildu slēptie saņēmēji vai failam nav reģistrētas atkārtotas lejupielādes).
- **riska ierobežošana un seku mazināšana:** tiek vērtēta iespēja atsaukt nosūtīto e-pastu vai bloķēt piekļuvi failam. Paralēli tiek uzsākta komunikācija ar datu saņēmēju, pieprasot datus nekavējoties dzēst, tos neizmantot un sniegt organizācijai skaidru, rakstisku apliecinājumu par datu iznīcināšanu.

Piemēram, iestādes darbinieks kļūdas dēļ uz ārēja pakalpojuma sniedzēja e-pasta adresi nosūta excel failu, kurā ir informācija par 500 personām, tostarp vārds, uzvārds, personas kods un kontaktinformācija.

Izmeklēšanas sākumā tiek noskaidrots, **kam tieši fails nosūtīts un vai tas faktiski ir piegādāts saņēmējam**. Tiek pārbaudīti e-pasta žurnālfaili, lai noskaidrotu saņēmēja adresi, nosūtīšanas laiku un to, vai e-pastam nav bijuši citi saņēmēji. Ja tehniski iespējams, tiek pārbaudīts arī, vai saņēmējs e-pastu ir atvēris vai failu lejupielādējis.

Pēc tam tiek izvērtēts, **kādi dati saņēmējam faktiski bija pieejami**. Piemēram, ja failā bija tikai 500 personu vārdis un tālruņa numuri, risks var būt atšķirīgs no situācijas, kurā tajā pašā failā bija arī personas kodi, informācija par veselību vai finanšu dati. Tiek noskaidrots arī, vai fails ir bijis pieejams

tikai vienam saņēmējam vai arī tas ir pārsūtīts citām personām.

Tālāk tiek vērtēts, **vai incidenta sekas vēl ir iespējams ierobežot**. Piemēram, ja saņēmējs vēl nav atvēris e-pastu, var būt iespējams atsaukt tā nosūtīšanu vai bloķēt piekļuvi failam. Ja saņēmējs failu jau ir saņēmis, ar viņu nekavējoties sazinās un lūdz failu dzēst, to nepārsūtīt un neizmantot. Ja iespējams, tiek lūgts arī apliecināt, ka fails un tajā ietvertie dati ir dzēsti un nav saglabāti citā veidā.

Vienlaikus tiek fiksēti visi būtiskie fakti – **cik personu dati ir skarti, kādi datu veidi ir izpausti, kam dati kļuvuši pieejami, vai tie ir atvērti vai lejupielādēti un vai pastāv iespēja, ka tie ir tālāk izplatīti**. Ja incidenta izmeklēšanas laikā tiek konstatēts, ka fails ir pārsūtīts vēl citām personām, attiecīgi tiek paplašināts arī incidenta tvērums.

Visbeidzot, **pamatojoties uz noskaidrotajiem faktiem un veiktajiem riska mazināšanas pasākumiem, tiek novērtēts risks skarto personu tiesībām un brīvībām**. Piemēram, situācija, kurā kļūdaini nosūtīts fails nekavējoties tiek dzēsts, to ir saņēmis tikai viens saņēmējs un nav pierādījumu par tā atvēršanu vai tālāku izplatīšanu, būs vērtējama citādi nekā situācija, kurā fails ir lejupielādēts, pārsūtīts vairākām personām un saturējis sensitīvu informāciju par lielu skaitu personu. Tieši šie apstākļi tiek ņemti vērā, pieņemot lēmumu par nepieciešamību paziņot par pārkāpumu Inspekcijai un informēt skartās fiziskās personas (datu subjektus).

Piemēram, uzņēmums "Datiņš" tirgo sadzīves tehniku internetā. Darbinieks gatavo e-pastu preču piegādātājam, lai pasūtītu 20 kafijas automātus un 10 putekļsūcējus. E-pastam jāpievieno Excel fails ar pasūtāmo preču sarakstu, taču darbinieks kļūdas dēļ pievieno citu failu, proti, uzņēmuma klientu sarakstu, kurā ir 500 klientu vārdi, uzvārdi, personas kodi un tālruņa numuri. Aptuveni pēc stundas darbinieks pamana kļūdu un par to nekavējoties ziņo uzņēmumā atbildīgajam darbiniekam. Uzņēmums noskaidro, ka e-pasts nosūtīts vienam piegādātāja darbiniekam. Ar viņu sazinās, un saņēmējs apliecina, ka failu ir atvēris, bet nav to pārsūtījis vai citādi izmantojis un pēc uzņēmuma lūguma to izdzēš. Uzņēmums fiksē noskaidrotos apstākļus un izvērtē incidenta radīto risku, ņemot vērā to, kādi dati izpausti, cik cilvēku dati ir skarti, kam tie kļuvuši pieejami un kādi pasākumi veikti, lai mazinātu iespējamās sekas.

2) Informācijas iegūšana integritātes pārkāpumu gadījumos.

Ja konstatēts integritātes pārkāpums, galvenais fokuss ir saprast, kas tieši un cik plaši ir izmainīts organizācijas rīcībā esošajos datos, kā arī vai un kā datus var droši atgriezt sākotnējā stāvoklī. Izmeklēšanas gaitā tiek veiktas šādas darbības:

- **izmaiņu avota un laika noteikšana:** tiek analizēti sistēmu žurnālfaili un ierakstu izmaiņu vēsture, lai precīzi atrastu brīdi, no kura dati kļuvuši nepareizi, un noteiktu izmaiņu veicēju (konkrēts lietotāja konts, automatizēts process, sistēmu integrācijas defekts vai kļūdains skripts).
- **skarto ierakstu kopas identificēšana:** tiek noteikts kļūdas mērogs - vai ietekmēti viena klienta dati, vai arī kļūda skar plašu datu bāzes segmentu (piemēram, visi klienti, kuriem konkrētais datu lauks satur kļūdainu vērtību).
- **datu atjaunošanas plāna izstrāde:** tiek noskaidrots, vai pastāv uzticama datu kopija (rezerves kopijas, drukāti līgumi, e-pastu sarakste vai vecākas sistēmas versijas), un pieņemts lēmums par labošanas metodi (manuāla datu korekcija vai labojoša skripta izstrāde).

- **seku un kaitējuma izvērtēšana:** tiek analizēts, vai kļūdaino datu dēļ jau ir iestājušās negatīvas sekas, piemēram, nosūtīti nepareizi rēķini, pieņemti tiesiski kļūdaini lēmumi vai pārkāpti līguma nosacījumi.

Piemēram, uzņēmums konstatē, ka tā klientu informācijas sistēmā vairākiem simtiem klientu ir mainīta deklarētā adrese. Sākotnēji nav zināms, vai adreses ir mainījuši paši klienti, uzņēmuma darbinieki, automatizēts process vai arī dati sistēmā nonākuši kļūdaini no citas sistēmas.

Izmeklēšanas sākumā tiek noskaidrots, kad tieši dati kļuvuši neprecīzi un cik klientu dati ir skarti. Sistēmas žurnālfailos un izmaiņu vēsturē tiek pārbaudīts, kad adreses mainītas un no kura lietotāja konta vai automatizēta procesa veiktas izmaiņas. Piemēram, izmeklēšanā var noskaidrot, ka 15. augustā plkst. 02.00 naktī vienas stundas laikā mainījušās 1200 klientu adreses un visas izmaiņas veicis viens un tas pats automatizēts process.

Tālāk tiek pārbaudīts, kāpēc automatizētais process veicis šīs izmaiņas. Tiek analizēts, no kuras sistēmas dati saņemti, vai nav izmantots kļūdains datu fails vai nepareizi konfigurēta integrācija. Piemēram, var tikt konstatēts, ka naktī veikta datu apmaiņa ar citu sistēmu un tās kļūdainas konfigurācijas dēļ klientu faktiskās adreses aizstātas ar tehniskām adresēm.

Pēc tam tiek identificēti visi skartie klientu ieraksti. Tiek noskaidrots, vai kļūda skar tikai 1200 klientu adreses vai arī tās rezultātā izmainīti citi personas dati. Vienlaikus tiek pārbaudīts, vai ir pieejama uzticama informācija par datu sākotnējo stāvokli, piemēram, rezerves kopija, iepriekšējā datubāzes versija vai dokumenti, kuros norādītas klientu pareizās adreses.

Kad kļūdas cēlonis un skarto datu apjoms ir noskaidrots, tiek sagatavots datu atjaunošanas plāns. Piemēram, ja ir pieejama iepriekšējās dienas rezerves kopija, no tās var atjaunot pareizās adreses. Ja rezerves kopija nav pieejama, var izmantot citu uzticamu datu avotu vai izstrādāt labojošu skriptu, kas atjauno tikai kļūdaini izmainītos ierakstus.

Paralēli tiek vērtēts, kādas sekas nepareizie dati jau ir radījuši. Piemēram, ja kļūdainās adreses tika izmantotas rēķinu vai citu paziņojumu nosūtīšanai, daļa klientu varēja nesaņemt tiem paredzēto informāciju. Ja dati tika izmantoti lēmumu pieņemšanai vai līgumsaistību izpildei, var būt nepieciešams pārbaudīt, vai šī kļūda nav izraisījusi arī citus pārkāpumus vai nelabvēlīgas sekas klientiem.

Visbeidzot, pamatojoties uz noskaidrotajiem faktiem, tiek izvērtēts risks skarto personu tiesībām un brīvībām un nepieciešamās turpmākās darbības. Tiek ņemts vērā gan skarto personu skaits un kļūdaini izmainīto datu veids, gan kļūdas ilgums, iespējamās sekas un tas, cik ātri un pilnīgi nepareizos datus iespējams atjaunot. Ja konstatēts personas datu aizsardzības pārkāpums, uz šī izvērtējuma pamata tiek pieņemts arī lēmums par nepieciešamību paziņot par pārkāpumu Inspekcijai un, ja nepieciešams, informēt skartās fiziskās personas.

Piemēram, SIA "Datiņš un partneri" ir interneta veikals, kas klientu profilā glabā viņu norādītās piegādes adreses. Kādu rītu uzņēmums saņem vairāku klientu ziņas, ka viņu profilā norādīta nepareiza adrese. Pārbaudot sistēmu, atklājas, ka nepareizas adreses ir vairāk nekā 1000 klientu profilos. Uzņēmums sāk pārbaudīt, kas noticis, un noskaidro, ka iepriekšējā naktī sistēmā automātiski veikta klientu datu atjaunošana. Tehniskas kļūdas dēļ daļai klientu iepriekš norādītās adreses aizstātas ar citu klientu adresēm. Uzņēmums noskaidro, kuri klienti ir skarti, aptur kļūdaino datu atjaunošanas procesu un no iepriekšējās dienas rezerves kopijas atjauno pareizās adreses. Vienlaikus tiek pārbaudīts, vai laikā, kamēr sistēmā bija nepareizās adreses, tās jau nav izmantotas, piemēram, preču nosūtīšanai. Pārbaudē tiek noskaidrots, ka 25 klientu pasūtījumi jau nodoti kurjeram, izmantojot

kļūdainās adreses. Uzņēmums sazinās ar kurjeru, lai apturētu šo sūtījumu piegādi, un izvērtē, kādas sekas incidents varētu radīt skartajiem klientiem un kādas turpmākās darbības nepieciešamas.

3) Informācijas iegūšana pieejamības pārkāpumu gadījumos

Ja konstatēts pieejamības pārkāpums, galvenais fokuss ir saprast, cik ilgi, kurām sistēmām un kurām personām dati vai pakalpojums nav bijis pieejams, kāda bijusi šīs nepieejamības ietekme un vai datus ir iespējams pilnībā atjaunot. Izmeklēšanas gaitā tiek veiktas šādas darbības:

- **dīkstāves hronoloģijas fiksēšana:** tiek analizēti sistēmu statusa ziņojumi un notikumu žurnāli, lai precīzi aprēķinātu reālo laiku, kurā sistēma vai dati nebija pieejami, kas ir kritiski svarīgi riska novērtēšanai.
- **cēloņa un rezerves kopiju audita veikšana:** tiek noskaidrots incidentu izraisījušais iemesls (tehnisks defekts, nejauša dzēšana cilvēka kļūdas dēļ vai mērķtiecīgs ļaunprātīgs uzbrukums, piemēram, *ransomware*). Speciālisti pārbauda pieejamās rezerves kopijas, nosaka, no kura brīža datus ir iespējams atjaunot un cik daudz pēdējo datu neizbēgami tiks zaudēts dīkstāves dēļ.
- **vai izdevies ievērot plānoto maksimāli pieļaujamo laiku, cik ilgi sistēma var būt nepieejama (RTO)[1] mērķi?**
- **reālās ietekmes vērtēšana uz datu subjektiem:** tiek analizēts, ko šī nepieejamība praktiski nozīmē fiziskajām personām - vai ir kavēti vai pārtraukti būtiski pakalpojumi (piemēram, veselības aprūpe, sociālie pakalpojumi, finanšu darījumi) vai citu tiesību īstenošana, kā arī novērtēta ietekme uz organizācijas reputāciju.

Piemēram, veselības aprūpes iestāde konstatē, ka tehniska incidenta dēļ nav iespējams piekļūt pacientu informācijas sistēmai. Sistēmā glabājas pacientu personas dati, informācija par iepriekšējām vizītēm, diagnozēm, nozīmētajām zālēm un izmeklējumu rezultātiem. Sistēmas nepieejamības dēļ ārstniecības personāls nevar piekļūt šai informācijai.

Izmeklēšanas sākumā tiek precīzi noskaidrots, **kad sistēma kļuvusi nepieejama un cik ilgi tā nav bijusi pieejama**. Piemēram, žurnālfailu analīze var parādīt, ka sistēmas darbība pārtraukta 8.00 un pilnībā atjaunota tikai 14.30. Tādējādi tiek konstatēts, ka pacientu dati sešarpus stundas nav bijuši pieejami.

Tālāk tiek noskaidrots, **kādi dati faktiski nav bijuši pieejami un vai tos iespējams atjaunot**. Tiek pārbaudītas rezerves kopijas un arhīvi, lai pārliecinātos, ka sistēmā glabātie dati nav zaudēti. Piemēram, var tikt konstatēts, ka pēdējā derīgā rezerves kopija izveidota iepriekšējās nakts laikā un pēc sistēmas atjaunošanas visi dati ir pilnībā pieejami. Ja rezerves kopija būtu bojāta vai novecojusi, būtu jānoskaidro, vai un cik daudz datu neatgriezeniski zaudēts.

Vienlaikus tiek noskaidrots **incidenta cēlonis**. Tiek pārbaudīts, vai sistēmas nepieejamību izraisījis tehnisks defekts, piemēram, servera vai datubāzes kļūme, cilvēka kļūda, piemēram, nejauša datu vai sistēmas konfigurācijas dzēšana, vai arī ārējs ļaunprātīgs uzbrukums. Ja konstatēts kiberuzbrukums, izmeklēšanā papildus jāpārbauda, vai uzbrucējs nav ne tikai padarījis sistēmu nepieejamu, bet arī

[1] RTO nozīmē Recovery Time Objective - maksimāli pieļaujamais laiks, cik ilgi sistēma drīkst būt nepieejama pēc incidenta vai katastrofas, līdz tās darbība jāatjauno.

piekļuvis tajā glabātajiem personas datiem.

Pēc tam tiek vērtēts, **kā sistēmas nepieejamība faktiski ietekmējusi pacientus**. Piemēram, ja incidenta laikā ārstiem nebija pieejama informācija par pacientu iepriekšējām diagnozēm vai nozīmētajām zālēm, jānoskaidro, vai tas ir ietekmējis ārstniecības procesu. Tāpat tiek pārbaudīts, vai pacientiem incidenta dēļ nav nācies atlikt vizītes, izmeklējumus vai ārstēšanu.

Ja sistēmas nepieejamības laikā bija iespējams izmantot alternatīvus risinājumus, piemēram, papīra dokumentāciju vai citu informācijas sistēmu, tiek vērtēts, **cik lielā mērā šie risinājumi mazinājuši incidenta ietekmi**. Piemēram, ja ārstiem bija pieejami iepriekš izdrukāti pacientu dati, bet tikai daļai pacientu, risks var būt mazāks nekā situācijā, kurā nebija pieejama nekāda alternatīva informācija.

Visbeidzot, **pamatojoties uz noskaidrotajiem faktiem, tiek izvērtēts risks skarto personu tiesībām un brīvībām**. Tiek ņemts vērā sistēmas nepieejamības ilgums, skarto personu skaits, nepieejamo datu raksturs, iespēja datus atjaunot, izmantotie alternatīvie risinājumi un faktiskās sekas pacientiem. Piemēram, sešas stundas ilga sistēmas nepieejamība, kuras laikā visi dati bija atjaunojami un ārstiem bija pieejami alternatīvi informācijas avoti, būs vērtējama citādi nekā vairāku dienu ilga nepieejamība, kuras dēļ pacientiem faktiski tika kavēta būtiska ārstniecības pakalpojumu saņemšana. Uz šī izvērtējuma pamata tiek noteiktas nepieciešamās turpmākās darbības, tostarp, ja piemērojams, lēmums par paziņošanu Inspekcijai un skartajām fiziskajām personām.

Piemēram, veselības centrā "Ārstē 123" darba dienas rītā plkst. 8.00 pārstāj darboties pacientu informācijas sistēma. Ārsti nevar apskatīt pacientu iepriekšējo vizīšu informāciju, diagnozes, nozīmētās zāles un izmeklējumu rezultātus. Tajā rītā veselības centrā ir pierakstīti 150 pacienti. Tehniskā pārbaude atklāj, ka bojājies serveris un sistēmas darbību iespējams atjaunot tikai plkst. 14.30. Dati nav pazaudēti un pēc sistēmas darbības atjaunošanas atkal ir pieejami pilnā apjomā. Kamēr sistēma nedarbojas, daļu pacientu ārsti var pieņemt, izmantojot iepriekš pieejamo informāciju un papīra dokumentus. Tomēr vairākiem pacientiem vizītes nākas pārcelt, jo ārstam bez sistēmā esošajiem izmeklējumu rezultātiem nav iespējams pieņemt lēmumu par turpmāko ārstēšanu. Piemēram, pacientam, kurš ieradies pie kardiologa, ārsts nevar apskatīt iepriekšējā dienā veikto izmeklējumu rezultātus, tādēļ vizīte tiek pārcelta uz nākamo dienu. Veselības centrs fiksē, cik ilgi sistēma nebija pieejama, cik pacientu tas skāra un kādas sekas radās, un, ņemot vērā šos apstākļus, izvērtē incidenta radīto risku un nepieciešamās turpmākās darbības.

Lai nodrošinātu vienotu un izsekojamu izmeklēšanas procedūru, organizācijai ir ieteicams standartizēt informācijas ieguves procesu (piemēram, izstrādājot iekšējo kontrolsarakstu vai izmeklēšanas formu). Tas garantē, ka katrā incidenta gadījumā neatkarīgi no tā specifikas tiks secīgi noskaidrots un dokumentēts pilns pamata faktoru kopums:

- **apjoms** (skarto personu skaits un datu lauku apjoms);
- **cēlonis** (cilvēkfaktors, sistēmas darbības kļūda vai mērķtiecīgs uzbrukums);
- **precīza notikumu secība** (hronoloģiskā laika līnija);
- **nepieciešamie papildu pasākumi** (tehniskie un organizatoriskie uzlabojumi).

Organizācija var izvēlēties savai darbībai un tehnisko rīku bāzei atbilstošāko risinājumu – tā var būt vienota struktūras datne (veidlapa), kurā neatkarīgi no pārkāpuma veida tiek sniegtas atbildes uz nemainīgu jautājumu kopu, un kas dinamiski tiek papildināta ar specifiskajām sadaļām, vai arī specializēts incidentu pārvaldības sistēmas modulis.

Standartizētas metodoloģijas izmantošana nodrošina, ka izmeklēšanas gaitā netiek izlaists neviens būtisks aspekts un ka visi noskaidrotie fakti un tehniskie pierādījumi kalpos par objektīvu pamatu galīgā riska līmeņa novērtēšanai (atbilstoši 2.5. nodaļai). Ilgtermiņā šāda pieeja sniedz organizācijai iespēju strukturēti salīdzināt dažādus incidentus savā starpā, identificēt sistēmiskas vājības un nodrošināt juridiski dzelžainu, izsekojamu pamatojumu uzraudzības iestādei par organizācijas pieņemtajiem gala lēmumiem.

2.3. Izvērtēt, vai ieviestie pasākumi bija pietiekami incidenta novēršanai vai ierobežošanai

Sasniedzamais rezultāts
Skaidri dokumentēts secinājums par to, kuri drošības pasākumi incidenta laikā bija efektīvi un kuri izrādījās nepietiekami. Pamatojoties uz šo izvērtējumu, tiek noteikti konkrēti uzlabojumi, kas jāievieš, lai līdzīgi incidenti mazinātos vai tiem būtu mazāka ietekme.

Veicamie pasākumi

Šīs darbības mērķis ir sistemātiski fiksēt secinājumus par to, cik efektīvi strādā ieviestie drošības pasākumi incidenta laikā, kur tie izrādījās nepietiekami un kādi uzlabojumi ir nepieciešami, lai līdzīgi gadījumi nākotnē vai nu vairs neatkārtotos, vai arī to ietekme būtu mazāka.

Lai šo soli veiktu jēgpilni, vispirms ir jāidentificē, kuri tieši drošības pasākumi ir būtiski konkrētajam incidentam (skatīt šo vadlīniju II. nodaļu "Tehniskie un organizatoriskie pasākumi personas datu drošības nodrošināšanai").

Piemēram, ja incidents ir saistīts ar pazudušu portatīvo datoru, uzmanība jāpievērš šifrēšanai, paroļu politikai un iespējai attālināti bloķēt vai dzēst ierīci.

Ja incidents radies tādēļ, ka e-pasts nosūtīts nepareizam adresātam, jāizvērtē darbinieku apmācības, e-pasta sūtīšanas procedūras un iespējamie tehniskie drošības risinājumi (piemēram, brīdinājumi par sūtīšanu ārpus organizācijas, divpakāpju apstiprinājums jutīgiem pielikumiem).

Ja incidents ir datu zudums, uzmanības centrā nonāk rezerves kopiju esamība, to regularitāte un atjaunošanas plāns.

Tālāk tiek pārbaudīts, vai attiecīgie pasākumi incidenta brīdī patiešām bija ieviesti un piemēroti, vai darbinieki tos izmantoja pareizi un vai bija atbilstoši konkrētajam incidentam. Fakts, ka parole tehniski pastāv, nenozīmē, ka pasākums ir pietiekams, ja parole ir ļoti vāja vai vienāda visiem darbiniekiem, vai arī, ja ir izstrādāti noteikumi,kādai parolei ir jābūt, bet darbinieki par to nezina vai to sistemātiski neievēro, tad šis pasākums ir formāls un neatbilstošs.

Beigās ir būtiski secinājumus skaidri dokumentēt, formulējot, ka konkrētais pasākums bija pietiekams vai nepietiekams un kāpēc, kā arī norādot, kādi uzlabojumi nepieciešami. Piemēram, kādi jauni risinājumi jāievieš vai kuri esošie jāpastiprina. Šie secinājumi vēlāk kalpo kā pamats korektīvajiem un preventīvajiem pasākumiem, kas tiek pievienoti incidenta lietai un drošības uzlabošanas plānam.

2.4. Reģistrēt visus aizdomīgos vai apstiprinātos gadījumus Incidentu reģistrā

Sasniedzamais rezultāts
Izveidots un regulāri uzturēts Incidentu reģistrs, kurā konsekventi tiek fiksēti visi aizdomīgie un apstiprinātie incidenti, tai skaitā PDAP.

Veicamie pasākumi
Incidentu reģistrs ir dokuments, kurā tiek apkopota visa būtiskā informācija par PDAP. Par reģistra uzturēšanu atbild viena vai vairākas personas, un reģistrs praktiski var būt gan Excel vai Word, gan specializēta sistēma. Būtiski ir nodrošināt, lai tas būtu pieejams un vienmēr aktuāls. Tajā vismaz tiek fiksēts incidenta:

- atklāšanas datums un laiks;
- īss apraksts;
- iesaistīto personas datu kategorijas;
- aptuvenais skarto datu subjektu skaits;
- incidenta avots;
- incidenta klasifikācija;
- sākotnējais un galīgais riska novērtējums;
- lēmumi par ziņošanu vai neziņošanu Inspekcijai un datu subjektiem;
- veiktie pasākumi;
- incidenta statuss (atvērts, izmeklēšanā, slēgts);
- atbildīgā persona.

Svarīgi, ka reģistrā tiek iekļauti ne tikai tie PDAP, par kuriem ziņots Inspekcijai, iesaistītajām fiziskajām personām, bet arī šķietami ikdienišķie gadījumi un pat situācijas, kas sākotnēji izskatījās pēc incidenta, bet izrādījās maldīga trauksme. Šādos gadījumos reģistrā skaidri norāda, ka izvērtējuma rezultātā secināts, ka nav PDAP vai nav nepieciešama ziņošana, tas vēlāk ļauj pamatot, kāpēc konkrētā situācijā netika veiktas papildu darbības.

Regulāri uzturēts Incidentu reģistrs palīdz sagatavot informāciju gan organizācijas vadībai, gan arī pamatot pieņemtos lēmumus Inspekcijai, kā arī identificēt atkārtotus cēloņus un tendences. Piemēram, bieži nepareizi nosūtītus e-pastus vai problēmas ar piekļuves tiesībām, no kā var plānot konkrētus drošības un procesu uzlabojumus.

3. solis

Personas datu aizsardzības pārkāpuma ietekmes (I) novērtēšana

Mērķis: novērtēt iespējamo ietekmi uz datu subjektiem (fizisku, materiālu vai nemateriālu).

Sasniedzamais rezultāts
Sistemātiski un objektīvi novērtēt incidenta iespējamo negatīvo ietekmi uz fizisko personu tiesībām un brīvībām (fizisku, materiālu vai nemateriālu kaitējumu, piemēram, identitātes zādzību, finansiālus zaudējumus vai reputācijas kaitējumu). Šis novērtējums ir obligāts juridisks pamats lēmuma pieņemšanai par ziņošanu uzraudzības iestādei (Datu regulas 33. pants) un pašu datu subjektu informēšanai (Datu regulas 34. pants).

Veicamie pasākumi
Datu regulas 33. pants nosaka organizācijai pienākumu informēt uzraudzības iestādi ne vēlāk kā 72 stundu laikā kopš brīža kad kļuvis zināms par pārkāpumu, izņemot gadījumus, kad ir maz ticams, ka PDAP varētu radīt risku fizisku personu tiesībām un brīvībām. Tas nozīmē, ka Datu regulas

33. panta izpilde ir saistāma ar notikuša PDAP risku novērtējumu, paziņošanas pienākumam parādoties gadījumā, ja risku iestāšanās ir mazticama.

Datu regulas 34. pants nosaka pienākumu personas datu pārkāpuma gadījumā informēt arī datu subjektu gadījumos, ja PDAP rada augstu risku datu subjekta tiesībām un brīvībām. Arī šī pienākuma izpilde ir saistīta ar organizācijas veiktu risku novērtējumu.

Riski datu subjekta tiesībām un brīvībām var izrietēt ne tikai no konfidencialitātes pārkāpuma, bet arī no pieejamības un integritātes pārrāvumiem. Abos šajos gadījumos gan atšķirsies faktori, kas ņemami vērā ietekmes novērtēšanai, tomēr abos gadījumos, konstatējot riskus, ir nepieciešams pildīt pienākumu attiecībā informēšanu par datu aizsardzības pārkāpumu.

Ietekmes noteikšanas metodika (ENISA pieeja)

Lai riska novērtējums nebūtu subjektīvs minējums, organizācija var izmantot Eiropas Savienības Kiberdrošības aģentūras (ENISA) izstrādāto un starptautiski atzīto metodiku. Šajā nodaļā aprakstītā ENISA metodika ir rekomendējošs un starptautiski atzīts rīks objektīva riska noteikšanai. Organizācija ir tiesīga izmantot arī savu iekšēji izstrādātu risku novērtēšanas metodoloģiju, taču tajā jebkurā gadījumā obligāti ir jābūt iestrādātiem pamata kritērijiem: datu raksturam (finanšu, īpašo kategoriju u.c.), identifikācijas vieglumam, kontekstam un tam, vai dati bijuši uzbrukuma mērķis vai, tieši otrādi, bijuši aizsargāti ar šifrēšanu/pseidonimizāciju (atstājot atslēgas neskartas), kas potenciālo ietekmi mazinātu.

Ietekmes līmenis (*I*) tiek aprēķināts, kombinējot trīs galvenos elementus:

Ietekmes līmenis (I) = Datu apstrādes konteksts (DAK) x Identifikācijas vieglums (IV) + Incidenta apstākļi (IA)

Lai veiktu šo aprēķinu, par izmeklēšanu atbildīgā persona secīgi iziet trīs soļus, piešķirot atbilstošos punktus.

3.1. Datu apstrādes konteksta (DAK) noteikšana

Pirmajā solī noteic, cik jutīgi pēc savas būtības ir incidentā iesaistītie personas dati un kāds ir to konteksts. Vērtēšana sākas ar bāzes līmeņa noteikšanu, ko pēc tam koriģē ar ietekmi palielinošiem vai mazinošiem faktoriem.

A. DAK bāzes līmeņi:

- **1 punkts – zems (ikdienas dati):** vārds, uzvārds, e-pasts, tālruņa numurs, pasta adrese.
- **2 punkti – vidējs (uzvedības dati):** profilēšanas dati, tīmekļa pārlūkošanas vēsture, ģeolokācija, klientu lojalitātes un pirkumu vēsture.
- **3 punkti – augsts (finanšu dati):** kredītkaršu numuri, bankas kontu izraksti, nodokļu informācija, algu dati un darba samaksas saraksti.
- **4 punkti – kritisks (īpašu kategoriju dati):** medicīniskie dati, slimības vēsture, ģenētiskie dati, sodāmības un pārkāpumu dati, kā arī nacionālie unikālie identifikatori (personas kodi).

B. Faktori, kas paaugstina DAK vērtību:

Pat ja dati pēc būtības ir ikdienišķi, to DAK vērtību var paaugstināt (līdz pat maksimālajiem 4 punktiem) šādi specifiski apstākļi:

1. **Datu apjoms (attiecībā uz vienu personu):** ja informācijas apjoms ir liels laika vai satura izteiksmē.

- *Laika aspekts:* viena gada datu vēstures noplūde rada lielāku ietekmi nekā vienas nedēļas datu noplūde.
- *Satura aspekts:* pilna bankas klienta lieta rada smagāku ietekmi nekā viens atsevišķs dokuments no šīs pašas lietas.

2. **Datu pārziņa darbības jomas specifika:** ja pārziņa darbības raksturs atklāj papildu sensitīvu informāciju par personu.
   - *Piemērs:* klientu saraksta (vārds, uzvārds) noplūde no kancelejas preču veikala ir ar DAK vērtību 1. Turpretim tāda paša saraksta noplūde no **plastiskās ķirurģijas klīnikas** vai **tiešsaistes aptiekas** nekavējoties paaugstina DAK uz **4**, jo atklāj ziņas par personu veselību vai privāto dzīvi.
3. **Datu subjektu īpašās pazīmes:** ja skartās personas pieder pie mazaizsargātām vai sociāli jutīgām grupām (piemēram, nepilngadīgie, bērni, personas ar īpašām vajadzībām vai specifisku juridisko statusu).
4. **Konteksta radītā papildu ietekme:** ziņas par to, ka persona ziedo līdzekļus, iegūst pavisam citu ietekmes smagumu, ja nolūks demonstrē atbalstu kādam politiskam virzienam vai piederību reliģiskajai organizācijai (kas ir politiskie vai reliģiskie uzskati kā īpašas kategorijas dati), salīdzinot ar ziedojumu dzīvnieku patversmei.

C. Faktori, kas samazina DAK vērtību:

Atsevišķos izņēmuma gadījumos bāzes DAK vērtību var samazināt, ja organizācijai ir skaidri pierādījumi par šādiem apstākļiem:

1. **Datu nederīgums vai neprecizitāte:** ja dati ir novecojuši vai kļūdaini, tādēļ to nozīme ir minimāla. *Piemērs:* pasta adrešu saraksts, uz kurām sūtījumus jau ilgstoši nav izdevies piegādāt (personas ir pārcēlušās).
2. **Iepriekšēja publiska pieejamība:** ja dati jau pirms incidenta bijuši likumīgi publicēti un ir viegli pieejami publiskos, oficiālos avotos.
3. **Datu ierobežotais raksturs:** ja konkrētā datu kopa, neraugoties uz formālo piederību sensitīvai kategorijai, nesniedz reālu informāciju par personas privāto dzīvi. *Piemērs:* Medicīniska izziņa, kas tikai sausi apliecina, ka "persona ir labā veselības stāvoklī", neatklājot nekādas diagnozes vai anamnēzi. Šādu DAK var samazināt no 4 uz 1, taču šis izņēmums jāpiemēro ar īpašu piesardzību un juridisku pamatojumu.

3.2. Identifikācijas viegluma (IV) noteikšana

Otrajā solī novērtē, cik viegli trešā persona vai uzbrucējs var sasaistīt noplūdušos datus ar konkrētu, dzīvu fizisku personu. IV koeficients tiek noteikts skalā no 0.25 līdz 1.00 atkarībā no datu veida un pieejamajiem palīglīdzekļiem. IV vērtības nesummējas, bet pēc noteikšanas ir jāpiemēro augstākā noteiktā IV vērtība. Ja atbilstoši kādam datu elementam jau ir piešķirama augstākā – 1.00 gradācija, tad citi datu elementi šo vērtību vairs nevar paaugstināt.

IV vērtības gradācija pa datu elementu grupām:

Datu elementi	**IV = 0.25 (Nenozīmīgs)**	**IV = 0.50 (Ierobežots)**	**IV = 0.75 (Būtisks)**	**IV = 1.00 (Maksimāls)**
Tiešie identifikatori (vārds, uzvārds)	Valsts mērogā, ja vārds/uzvārds ir ļoti bieži sastopams (piem., *Jānis Bērziņš*).	Valsts mērogā, ja vārds/uzvārds ir salīdzinoši reti sastopams.	Nelielas pilsētas vai organizācijas ietvaros, kur persona ir viegli atpazīstama.	Valsts mērogā, ja klāt ir papildu dati (dzimšanas datums, e-pasts).
Unikālie identifikatori (pase, ID, personas kods)	Ir tikai numurs, nav piekļuves valsts atsauces datubāzēm, lai uzzinātu vārdu.	*Identifikators pats atklāj datus (piemēram, personas kods atklāj dzimšanas datumu)*	Identifikators pats atklāj datus (piem., personas kods atklāj dzimšanas datumu) un ir kopā ar citu informāciju, piemēram, adresi.	Numurs ir kopā ar papildu identifikatoriem pilnu vārdu, uzvārdu un/vai personas fotogrāfiju un citu informāciju
Netiešie identifikatori (telefons, adrese u.c.)	Numurs/adrese nav reģistrēti nekādos publiskos reģistros.	Mazas pilsētas ietvaros (identifikācija iespējama, veicot kontrolzvanu).	*Netiešais identifikators saistīts ar citu informāciju, piemēram, viedokli par personu*	Netiešais identifikators ir brīvi atrodams publiskos reģistros vai internetā un ir saistīti ar citu informāciju
E-pasta adrese	Adrese neatklāj vārdu (piem., *kakis123@inbox.lv*) un nav izmantota sociālajos tīklos.	Adrese neatklāj vārdu, bet ir izmantota kā primārais lietotājvārds publiskos forumos/tīklos.	E-pasta adrese satur personas vārdu vai citu identificējošu informāciju (piem., janis1985@...), un, izmantojot publiski pieejamus avotus, to iespējams samērā viegli sasaistīt ar konkrētu	E-pasta adrese satur personas pilnu vārdu un uzvārdu (piem., janis.berzins@...) un pati par sevi vai kopā ar publiski pieejamu informāciju ļauj nepārprotami identificēt personu.

Datu elementi	IV = 0.25 (Nenozīmīgs)	IV = 0.50 (Ierobežots)	IV = 0.75 (Būtisks)	IV = 1.00 (Maksimāls)
			personu.	
Attēls/ fotogrāfija	Attēls ir neskaidrs, miglains (piem., videonovērošana no liela attāluma naktī).	Attēls ir miglains, bet satur kontekstu (apkārtni, specifisku formu, automašīnu).	Attēls ir pilnībā skaidrs, bet nav sasaistīts ar citiem teksta datiem.	Attēls ir skaidrs un sasaistīts ar papildu datiem (dzīvesvietu, vārdu, amatu).
Kodi/ pseidonīmi/ iniciāļi	Kods neatklāj personu un nav sasaistāms bez slepenās atsauces tabulas (atslēgas).	*Kods neatklāj personu, bet pastāv citi saprātīgi pieejami līdzekļi, ar kuriem teorētiski personu iespējams atklāt*	Pseidonīms vai iniciāļi atklāj daļu informācijas un ir kopā ar e-pasta adresi.	Pseidonīms tieši atklāj pilnu vārdu vai arī uzbrucējam ir pieejama atsauces datubāze.

Piemēram:

- Nenozīmīgs IV (0,10).

Incidenta sākotnējā izmeklēšanā konstatēts, ka ir iegūts tikai nejauši ģenerēts klienta identifikators, piemēram, K7F4-92QX. Identifikators pats par sevi nesatur informāciju par personu un bez organizācijas rīcībā esošās atsauces tabulas nav sasaistāms ar konkrētu personu. Tādēļ personas IV ir ļoti zems.

- Ierobežots IV (0,25).

Turpinot izmeklēšanu, noskaidrots, ka līdz ar identifikatoru ir iegūts arī klienta e-pasta lietotājvārds, piemēram, kakis123. Lai gan tas pats par sevi personu neidentificē, publiski pieejamā forumā atrodama informācija, kas šo lietotājvārdu sasaista ar konkrētu personu. Tādējādi personu jau ir iespējams identificēt, izmantojot saprātīgi pieejamu papildu informāciju, un IV palielinās.

- Būtisks IV (0,50).

Vēlāk konstatēts, ka uzbrucējam pieejams arī personas vārds un uzvārds, piemēram, Jānis Bērziņš, kā arī iepriekš minētais identifikators un e-pasta adrese. Persona vairs nav tikai netieši identificējama – pieejamo datu elementu kombinācija ļauj konkrēto datu subjektu identificēt bez būtiskas papildu izpētes.

- Ļoti augsts IV (0,75).

Turpmākā izmeklēšana atklāj, ka kompromitēta arī personas dzīvesvietas adrese un tālruņa numurs. Šo datu kombinācija ļauj personu nepārprotami identificēt un būtiski samazina nepieciešamību izmantot papildu informāciju identitātes noteikšanai.

- Maksimāls IV (1,00).

Noslēgumā tiek konstatēts, ka uzbrucējs ir ieguvis arī unikālu valsts izsniegtu identifikatoru, piemēram, personas kodu, kā arī personas fotogrāfiju un citus ar personu saistītus datus. Šajā situācijā konkrētās personas identitāti iespējams noteikt nepārprotami un ar minimālu papildu informāciju vai bez tās. Tādējādi IV sasniedz maksimālo novērtējuma līmeni - 1,00.

Tomēr jāatceras, ka pats apstāklis cik viegli personu identificēt datu kopā vēl pats par sevi nerada PDAP kopējo vērtību – tas ir tikai viens no kopējā aprēķina elementiem.

3.3. Personas datu aizsardzības pārkāpuma apstākļu (IA) ietekme

Trešajā solī aprēķinam pieskaita vai atņem punktus atkarībā no tā, kā tieši incidents ir noritējis un kādas sekas jau ir iestājušās.

Svarīgi ir tas, ka katrs konstatētais apstāklis tiek vērtēts neatkarīgi, un tie var summēties.

Konfidencialitātes zudums

- **0 punkti:** dati ir pakļauti riskam, bet nav nekādu pierādījumu, ka ir notikusi nelikumīga piekļuve. *Piemēram,* portatīvais dators pazaudēts aizslēgtā somā; servera aprīkojums utilizēts, pirms tam datus nepārrakstot, bet tas atrodas slēgtā poligonā.
- **+0.25 punkti:** dati ir nonākuši **zināma un ierobežota** skaita personu rīcībā. *Piemēr*am, e-pasts kļūdaini nosūtīts konkrētam sadarbības partnerim; pašapkalpošanās portāla kļūdas dēļ klients uz mirkli redzēja cita zināma klienta profilu.
- **+0.50 punkti:** dati ir nonākuši **nenoteikta skaita nezināmu un potenciāli ļaunprātīgu** saņēmēju rīcībā. *Piemēram,* dati publicēti atvērtā interneta forumā vai P2P vietnē; darbinieks nozagto datubāzi pārdevis trešajām personām; nepareizas IT konfigurācijas dēļ dati bijuši brīvi indeksējami *Google* meklētājā.

Integritātes zudums (datu izmainīšana)

- **0 punkti:** dati ir mainīti, bet nav izmantoti un ir pilnībā atjaunoti. *Piemēr*am, datubāzes ieraksti kļūdaini pārrakstīti, bet IT komanda pamanīja kļūdu un atjaunoja rezerves kopiju pirms sistēmu iedarbināšanas lietotājiem.
- **+0.25 punkti:** dati ir mainīti, pastāv risks, ka tie izmantoti nepareizi, taču tos **ir iespējams** atjaunot. *Piemēr*am, medicīniskajā profilā tiešsaistē ir izmainīti dati, sistēma darbojas kļūdaini un pacients ir spiests pakalpojumu kārtot manuāli, bezsaistē.
- **+0.50 punkti:** dati ir izmainīti, izmantoti kļūdaini un sākotnējo versiju **nav iespējams** atjaunot (zaudēti neatgriezeniski).

Pieejamības zudums (datu nepieejamība/ dīkstāve)

- **0 punkti:** datus iespējams atjaunot nekavējoties un bez grūtībām. *Piemēr*am, fails ir izdzēsts, bet IT uzreiz atjaunoja precīzu kopiju no paralēlā servera.

- **+0.25 punkti:** datu īslaicīga nepieejamība, kas prasa laiku atjaunošanai, vai arī subjektiem dati jāsniedz atkārtoti. *Piemēr*am, serveris ir bojāts, datu atjaunošana no rezerves kopijām aizņem 24 stundas, paralizējot klientu apkalpošanu.
- **+0.50 punkti:** pilnīga un neatgriezeniska nepieejamība. Rezerves kopiju nav, datus nav iespējams atgūt ne organizācijā, ne atkārtoti palūdzot no pašiem cilvēkiem.

Apzināts ļaunprātīgs nodoms un mērķis

- **+0.50 punkti:** pārkāpums ir noticis mērķtiecīgas, apzinātas rīcības rezultātā (ārējs kiberuzbrukums vai iekšēja sabotāža), lai nodarītu kaitējumu organizācijai vai pašiem cilvēkiem. Izmeklēšanas dati skaidri liecina, ka tieši šī konkrētā personas datu kopa bija **uzbrukuma primārais mērķis**.

Gala ietekmes līmeņa noteikšana un rīcības matrica

Saskaitot un sareizinot visus punktus pēc formulas (I = DAK x IV + IA), organizācija iegūst skaitli, kas nosaka tālāko rīcību.

Aprēķinātais I	**Ietekmes līmenis**	**Risks tiesībām**	**Nepieciešamā rīcība un ziņošana**
I mazāks vai vienāds ar 2	**Zems**	Mazticams	**Nav jāziņo ne DVI, ne iedzīvotājiem.** Incidents un tā izvērtējuma pamatojums tiek dokumentēts tikai iekšējā Incidentu reģistrā.
2 < I mazāks vai vienāds ar 3	**Vidējs**	Ticams riska iestāšanās gadījums	**Obligāti jāziņo Datu valsts inspekcijai 72 stundu laikā.** Paši iedzīvotāji (klienti) nav jāinformē.
3 < I mazāks vai vienāds ar 4	**Augsts**	Augsts risks	**Obligāti jāziņo gan DVI (72h laikā), gan nekavējoties jāinformē visi skartie cilvēki (datu subjekti)**.
I > 4	**Kritisks**	Ārkārtējs/ tūlītējs apdraudējums	**Tūlītēja krīzes vadība.** Ziņošana visām pusēm, sabiedrībai un tiesībsargājošajām iestādēm.

Piemērs- **personas datu aizsardzības incidenta apraksts**

Organizācijas informācijas sistēmā 2025. gada 15. augustā tika konstatēta nesankcionēta piekļuve datubāzei, kurā tika apstrādāti klientu personas dati. Izmeklēšanas gaitā tika noskaidrots, ka

nepiederoša persona, izmantojot kompromitētu lietotāja kontu, bija ieguvusi piekļuvi sistēmai un laika posmā no 6. līdz 15. augustam veikusi nesankcionētus datubāzes vaicājumus.

Incidenta rezultātā trešās personas rīcībā nonāca aptuveni 40 000 fizisku personu ieraksti. Katrā ierakstā bija ietverts personas vārds, uzvārds, personas kods, e-pasta adrese, tālruņa numurs un dzīvesvietas adrese. Daļā ierakstu bija pieejama arī informācija par personai piederošu transportlīdzekli.

Izmeklēšanā konstatēts, ka uzbrucējs nav tikai apskatījis sistēmā esošos datus, bet ir veicis ievērojama datu apjoma eksportu. Aptuveni 40 000 personu ierakstu tika lejupielādēti ārpus organizācijas informācijas sistēmas. Tā kā dati ir nonākuši nepiederošas personas kontrolē, organizācija šobrīd nevar pilnībā kontrolēt to turpmāku izmantošanu vai izplatīšanu.

Incidentā skartie dati ļauj personu identificēt tieši un bez būtiskas papildu informācijas. Turklāt datu kombinācija ļauj sasaistīt identificēto personu ar tās kontaktinformāciju, dzīvesvietu un konkrētu transportlīdzekli. Līdz ar to incidenta novērtējumā būtiska nozīme ir ne tikai atsevišķu datu elementu identificējamībai, bet arī to kopumam un datu apstrādes kontekstam.

Incidenta apstākļus pastiprina nesankcionētas piekļuves ilgums, skarto personu skaits un fakts, ka ievērojams datu apjoms ir faktiski izfiltrēts no organizācijas infrastruktūras.

Šajā gadījumā:

- DAK = 1,5 (pēc būtības noplūdušie dati ir ikdienas dati (1). Šo rādītāju var palielināt tas, ka noplūdušas arī ziņas par transportlīdzekli (šajā gadījumā +0,5), savukārt samazināt - tas, ja tiek konstatēts, ka ieraksti nav mašīnlasāmi);
- IV = 1 (jo zaudēts unikālais identifikators kopā ar papildu identifikatoriem un citu informāciju. Tā kā 1 ir maksimālā IV vērtība, pārējos elementus IV noteikšanā nav nepieciešams vērtēt);
- IA = 1 (jo +0,5 dati nonākuši ārpus pārziņa kontroles nezināma saņēmēju skaita rokās; +0,5 dati zaudēti mērķtiecīga uzbrukuma rezultātā);
- Ietekme = 1,5*1+1 (2,5). Ietekmes novērtējums var palielināties, ja tiek konstatēti papildu apstākļi. Piemēram, ja par vienu un to pašu personu saglabājušies vairāki ieraksti, kas ļauj spriest par tās paradumiem ilgākā laika posmā; ja informācija par transportlīdzekli var atklāt personas mantisko stāvokli; ja organizācijas darbības specifika var atklāt īpaša rakstura informāciju par personu (piemēram, tā ir ārstniecības iestāde); vai ja organizācija veic valsts pārvaldes funkcijas un personai ir īpašs pamats tai uzticēties.

!Paraugs: Personas datu pārkāpuma ietekmes novērtējuma veidlapa (skatīt pielikumā)

4. solis

Ziņošana (ja piemērojama)

Mērķis: savlaicīgi informēt uzraudzības iestādi un, ja nepieciešams, datu subjektus.

4.1. Saziņa ar uzraudzības iestādi (72 stundu noteikums)

Sasniedzamais rezultāts

Nodrošināta pilnīga Datu regulas 33. panta prasību izpilde, savlaicīgi un kvalitatīvi iesniedzot paziņojumu uzraudzības iestādei.

Veicamie pasākumi
Ja 3. solī veiktā riska novērtējuma rezultātā ir konstatēta vidēja, augsta vai kritiska ietekme (I > 2), organizācijai ir pienākums paziņot par pārkāpumu Inspekcijai ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tai kļuvis zināms.
Ja ziņošana šajā termiņā nav bijusi iespējama, paziņojumam ir jāpievieno kavējuma pamatojums (paziņošanu var veikt arī pa posmiem, ja visu informāciju uzreiz nav iespējams iegūt).

Paziņojums tiek iesniegts elektroniski, aizpildot oficiālo formu speciāli šim nolūkam paredzētajā DVI vietnē: https://pazinojums.dvi.gov.lv/. Savukārt, ja tiešsaistes formu kādu iemeslu dēļ aizpildīt nav iespējams, tad pārzinis var lejuplādēt iepriekš norādītajā saitē excel formu, aizpildīt to un iesniegt PDAP ar šīs excel formas starpniecību.

Tā kā šajā formā ir jāiekļauj informācija, kas jau secīgi apkopota iepriekšējos izmeklēšanas soļos (pārkāpuma cēlonis, laika līnija, skartie dati un subjektu kategorijas), šis solis ir iepriekšējā darba apkopojums.
Arī ja sākotnējā iesniegumā nav iespējams sniegt visu iesnieguma formā pieprasīto sistēmu, tad var norādīt to informāciju, kas ir pieejama, pārējās nepieciešamās ziņas papildinot pēc izmeklēšanas vai tās būtisku starpposmu noslēgšanās.

Inspekcijas informēšana nepieciešama galvenokārt tādēļ, lai:
1. mazinātu sistēmiskos riskus valstī, jo Inspekcija var novērtēt incidenta tehniskos cēloņus. Ja līdzīgai ievainojamībai ir pakļautas arī citas organizācijas, Inspekcija var centralizēti izplatīt brīdinājumus, lai mazinātu kiberapdraudējumus valsts mērogā.
2. novērtētu organizācijas spertos soļus, jo Inspekcija pārliecinās par organizācijas veiktajiem pasākumiem seku mazināšanā, ierobežošanā un izmeklēšanā, nepieciešamības gadījumā iesakot papildu drošības uzlabojumus.
3. salāgotu risku novērtējumu, jo Inspekcija pārliecinās, vai organizācijas veiktais riska vērtējums un izvēlētā stratēģija sakrīt ar uzraudzības iestādes redzējumu, pasargājot organizāciju no juridiskiem riskiem vēlākā posmā.
4. Aizsargātu personu intereses, jo Inspekcija palīdz nodrošināt, ka fizisko personu tiesības un intereses krīzes situācijā tiek aizsargātas maksimālajā apjomā.

4.2. Datu subjektu (fizisko personu) informēšana

Sasniedzamais rezultāts
Nodrošināta pilnīga Datu regulas 34. panta izpilde, sniedzot skartajiem cilvēkiem skaidru, savlaicīgu un saprotamu informāciju, kas dod viņiem iespēju operatīvi veikt pašaizsardzības pasākumus savu tiesību un interešu aizsardzībai.

Veicamie pasākumi
Ja riska novērtējums norāda uz augstu vai kritisku ietekmi (I > 3), organizācijai papildus ziņošanai DVI ir obligāts pienākums bez nepamatotas kavēšanās informēt arī pašus datu subjektus (klientus, darbiniekus).
Šis solis ir kritiski svarīgs, lai cilvēki, kuru dati ir kompromitēti, varētu nekavējoties rīkoties (piemēram, nomainīt paroles citos resursos, bloķēt bankas kartes, pastiprināti sekot līdzi aizdomīgiem darījumiem vai krāpnieciskiem e-pastiem/zvaniem).

Informēšanas veidi un kanāli
Organizācija izvēlas iedzīvotājiem efektīvāko un sasniedzamāko saziņas veidu:

- Individuāls paziņojums (primāri): ja skarto personu kontaktinformācija ir zināma un pieejama, katram cilvēkam tiek nosūtīts personīgs paziņojums (e-pasts, SMS vai ierakstīta vēstule).
- Publisks paziņojums (alternatīva): ja individuāla saziņa prasītu neproporcionāli lielas pūles vai izmaksas (piemēram, kontaktinformācija nav precīza vai skarto personu skaits mērāms tūkstošos), organizācija veic tikpat efektīvu publisku saziņu — publicē skaidru paziņojumu savā tīmekļa vietnē, sociālajos tīklos un/vai medijos.

Paziņojuma saturs (kas obligāti jāpasaka cilvēkiem)
Datu subjektam nosūtītajā informācijā jābūt izteiktai skaidrā, vienkāršā un viegli saprotamā valodā (bez sarežģītiem IT terminiem). Tajā obligāti iekļauj:

1) aprakstu par to, kas ir noticis (pārkāpuma raksturs un apstākļi);
2) datu aizsardzības speciālista vai cita kontaktpunkta koordinātas, kur var iegūt papildu informāciju;
3) aprakstu par iespējamām negatīvajām sekām, kas personai var rasties;
4) organizācijas jau veiktos vai plānotos pasākumus pārkāpuma novēršanai un seku mazināšanai;
5) praktiskus ieteikumus pašam datu subjektam, kādas darbības viņam šobrīd būtu vēlams veikt savas drošības stiprināšanai.

Piemērs iepriekš aprakstītajam PDAP ar pieņēmumu, ka tas radījis potenciālu augsta riska ietekmei uz datu subjektu- paziņojums par personas datu aizsardzības incidentu

Informējam, ka 2025. gada 15. augustā mūsu informācijas sistēmā konstatējām nesankcionētu piekļuvi datubāzei, kurā tika glabāti klientu personas dati. Izmeklēšanā noskaidrojām, ka nepiederoša persona, izmantojot nozagtu lietotāja piekļuvi, laikā no 6. līdz 15. augustam varēja piekļūt šiem datiem. Persona ne tikai apskatīja datus, bet arī lejupielādēja aptuveni 40 000 cilvēku ierakstus. Tas nozīmē, ka šie dati ir nonākuši ārpus mūsu informācijas sistēmas un mēs vairs nevaram pilnībā kontrolēt, kas ar tiem turpmāk var notikt.
Jūsu gadījumā incidentā varētu būt nonākuši **vārds, uzvārds, personas kods, e-pasta adrese, tālruņa numurs un dzīvesvietas adrese**. Daļai cilvēku datu bija pievienota arī informācija par viņiem piederošu transportlīdzekli. Šo datu kombinācija var ļaut nepiederošai personai ne tikai noskaidrot, kas esat, bet arī iegūt informāciju par to, kā ar Jums sazināties, kur dzīvojat un kāds transportlīdzeklis Jums pieder.
Šobrīd nav zināms, vai lejupielādētie dati jau ir izmantoti vai nodoti citām personām. Tomēr pastāv risks, ka tos var izmantot, piemēram, **krāpniecisku e-pastu, īsziņu vai telefona zvanu nosūtīšanai**, uzdodoties par organizāciju vai citu uzticamu personu. Tā kā noplūduši arī personas kods un dzīvesvietas adrese, pastāv arī risks, ka informācija var tikt izmantota, lai ticamāk uzdotos par Jums vai mēģinātu iegūt papildu informāciju par Jums.
Mēs esam nekavējoties ierobežojuši nesankcionēto piekļuvi, bloķējuši kompromitēto lietotāja kontu un veicam papildu pārbaudes, lai noskaidrotu visus incidenta apstākļus. Esam arī veikuši pasākumus, lai novērstu līdzīga incidenta atkārtošanos, un turpinām uzraudzīt sistēmas darbību. Ja izmeklēšanas gaitā iegūsim jaunu informāciju, kas var būt būtiska Jūsu drošībai, mēs Jūs par to informēsim.
Ko Jums ieteicams darīt? Īpaši aicinām turpmāk pievērst uzmanību negaidītiem e-pastiem, īsziņām un telefona zvaniem, kuros tiek prasīts atklāt paroles, internetbankas piekļuves datus, Smart-ID vai citus drošības kodus. Neatveriet aizdomīgas saites un nepārsūtiet citām personām saņemtos drošības kodus. Ja saņemat ziņu vai zvanu, kurā tiek izmantots Jūsu vārds vai cita informācija par Jums, bet tiek lūgts veikt kādu maksājumu vai atklāt piekļuves datus, vispirms patstāvīgi sazinieties ar attiecīgo iestādi vai pakalpojuma sniedzēju, izmantojot tā oficiālo kontaktinformāciju.
Ja izmantojat vienu un to pašu paroli vairākos pakalpojumos, iesakām to nomainīt un katram pakalpojumam izmantot atšķirīgu paroli. Ja Jums rodas aizdomas, ka kāds Jūsu datus jau izmanto

ļaunprātīgi, nekavējoties sazinieties ar attiecīgo pakalpojuma sniedzēju un, ja nepieciešams, tiesībsargājošajām iestādēm.
Ja Jums nepieciešama papildu informācija par incidentu vai vēlaties noskaidrot, vai tieši Jūsu dati ir bijuši incidentā iesaistīti, varat sazināties ar mūsu datu aizsardzības speciālistu: **[vārds, uzvārds, e-pasts, tālrunis]**.

!Paraugs: Datu subjekta informēšanas vēstules veidlapa (skatīt pielikumā).