Latvijas Republika
Izglītības un zinātnes ministrija

KANDAVAS LAUKSAIMNIECĪBAS TEHNIKUMS

Reģ. Nr. 90000032081
Valteru iela 6, Kandava, Kandavas novads, LV -3120,
tālr./fakss 63122502, e- pasts info@kandavastehnikums.lv

APSTIPRINU:
Kandavas Lauksaimniecības tehnikuma
direktore D.Rozentāle
2018. gada 31. oktobrī

Personas datu aizsardzības pārkāpumu atklāšanas, novēršanas un paziņošanas

KĀRTĪBA

I VISPĀRĪGIE NOTEIKUMI

1. Dokuments "Personas datu aizsardzības pārkāpumu atklāšanas, novēršanas un paziņošanas kārtība" (turpmāk – Kārtība) nosaka vienotu kārtību, kādā Sabiedrībā tiek veiktas darbības, lai atklātu, novērstu, reģistrētu personas datu aizsardzības pārkāpumus un normatīvajos aktos noteiktajos gadījumos veiktu paziņošanu par konstatētajiem pārkāpumiem Datu valsts inspekcijai un/vai Datu subjektam, kā arī novērstu šo pārkāpumu radītās sekas.

2. Šajā kārtībā ir lietoti šādi termini un saīsinājumi:

   2.1. **Pārzinis** – Kandavas Lauksaimniecības tehnikums (Tehnikums) Adrese: Valteru iela 6, Kandava, Kandavas novads, Latvija, LV-3120; tālr. 63122502; e-pasts: info@kandavastehnikums.lv ; interneta vietne: www.kandavastehnikums.lv.
   2.2. **Pārkāpums** – personas datu aizsardzības pārkāpums - drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, pazaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem;
   2.3. **Atbildīgās personas** – Dace Rozentāle, tel Nr. 26416920;
   2.4. **Regula** – Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK;
   2.5. **Reģistrs** – Notikumu reģistrs, kurā tiek reģistrēti visi Pārkāpumi;
   2.6. **Datu subjekts** – fiziska persona, kurai pārkāpuma rezultātā, tiek radīts augsts risks tās tiesībām un brīvībām.

2.7. **Vadlīnijas** - Kārtībai pielikumā pievienotas Vadlīnijas datu aizsardzības pārkāpumu atklāšanai, novēršanai un paziņošanai, kuru mērķis ir atvieglot šī dokumentu piemērošanu Pārziņa darbībā. Vadlīnijas izstrādātas pamatojoties uz Datu valsts inspekcijas norādījumiem un 29.panta darba grupas ieteikumiem. Vadlīnijās lietotajiem terminiem piemērojami šo noteikumu otrajā punktā minētie skaidrojumi.

Termini, kas nav definēti šajā punktā, tiek izmantoti atbilstoši to Regulā ietvertajai nozīmei.

Kārtība ir izdota, lai nodrošinātu Regulas 33. un 34.pantā noteiktā datu aizsardzības pārkāpumu paziņošanas pienākuma izpildi un attiecas gan uz automatizētā, gan manuālā veidā veiktu personas datu apstrādi, kā arī nodrošinātu indivīda tiesības uz datu aizsardzību Pārkāpuma gadījumā.

II DARBINIEKU PIENĀKUMI UN RĪCĪBA PĀRKĀPUMU GADĪJUMĀ

3. Visiem darbiniekiem ir pienākums iepazīties ar Vadlīnijām un zināt raksturīgākos Pārkāpumu veidus, to raksturīgākās pazīmes, veikt savas kompetences un iespēju robežās visas nepieciešamās darbības, lai novērstu un/vai pārtrauktu Pārkāpumus, novērstu vai mazinātu Pārkāpuma sekas, ziņot par Pārkāpumu Atbildīgajai personai.
4. Darbinieks, konstatējot Pārkāpumu vai pamatotu tā rašanās iespējamību, nekavējoties, bet ne vēlāk kā 8 stundu laikā, ziņo par to Atbildīgajām personām, norādot informāciju par Pārkāpumu, Pārkāpuma sekām, kā arī informāciju par darbībām, kas ir veiktas Pārkāpuma novēršanai, pārtraukšanai, Pārkāpuma seku novēršanai vai mazināšanai.
5. Darbiniekiem ir pienākums ziņot par konstatētajiem vai iespējamiem Pārkāpumiem, neatkarīgi no Pārkāpuma konstatēšanas veida: Pārkāpums radies paša Darbinieka rīcības rezultātā; Darbinieks pamanījis iespējamo Pārkāpumu saistībā ar cita Darbinieka rīcību; saņemot informāciju no datu subjekta; Pārziņa apstrādātājiem (sadarbības partneriem); saņemot publiski pieejamu informāciju; veicot Pārziņa pārbaudi vai auditu.
6. Darbinieks savas kompetences ietvaros veic visas iespējamās darbības, lai nepieļautu Pārkāpuma iestāšanos, pārtrauktu jau iestājušos pārkāpumu, kā arī, lai likvidētu vai mazinātu tā nelabvēlīgās sekas, vienlaikus rūpējoties par to, lai neiznīcinātu informāciju par vēlākam procesam svarīgiem apstākļiem (pierādījumiem). Šādā gadījumā ziņošana par iespējamo Pārkāpumu tiek veikta pēc darbību veikšanas, kas nepieciešamas iespējamā Pārkāpuma novēršanai vai pārtraukšanai un tā seku mazināšanai vai likvidēšanai.

III ABILDĪGĀS PERSONAS PIENĀKUMI UN RĪCĪBA PĀRKĀPUMA GADĪJUMOS PĀRKĀPUMU PAZIŅOŠANA

7. Atbildīgā persona:
   7.1. veic Pārkāpuma novēršanu, apturēšanu, seku novēršanu vai mazināšanu;
   7.2. uztur Reģistru un veic tajā informācijas papildināšanu/atjaunināšanu Kārtībā noteiktajos gadījumos;
   7.3. nepieciešamības gadījumā, nodrošina paziņošanu par Pārkāpumiem Datu valsts inspekcijai;
   7.4. veic citus Kārtībā, amata aprakstā, spēkā esošajos normatīvajos aktos noteiktos pienākumus.
8. Pēc informācijas par iespējamo Pārkāpumu saņemšanas Atbildīgās personas Pārkāpumu tajā pašā dienā reģistrē Reģistrā.
9. Atbildīgā persona, savas kompetences ietvaros, nekavējoties veic darbības, lai Pārkāpums tiktu novērsts vai pārtraukts un tiktu novērstas vai mazinātas tā rezultātā radušās sekas (ja tās nav veicis darbinieks, kurš ziņoja par Pārkāpumu).
10. Atbildīgā persona izvērtē, vai Pārkāpums var radīt risku datu subjekta tiesībām un brīvībām. Ja Atbildīgā persona konstatē, ka pastāv varbūtība, ka Pārkāpums var radīt risku datu subjektu tiesībām un brīvībām, tad Atbildīgā persona rakstveidā dokumentē savu slēdzienu, un iesniedz to Pārziņa direktoram.
11. Pārziņa direktors pēc Noteikumu 11.punktā minētā atzinuma saņemšanas nekavējoties to izskata. Ja Pārziņa direktors atzīst, ka Atbildīgā personas atzinums ir pamatots, tad direktors pieņem lēmumu par Pārkāpuma paziņošanu Datu valsts inspekcijai un/vai Datu subjektam/-iem, un uzdod to nodrošināt Atbildīgajai personai vai citai personai, atbilstoši šiem noteikumiem

12. Atbildīgās personas pieņemot slēdzienu (11.punkts) un Pārziņa direktors pieņemot galīgo lēmumu, jo īpaši ņem vērā sekojošus apstākļus, kā arī Vadlīnijas:
    12.1. Pārkāpuma radītais risks fizisku personu tiesībām un brīvībām;
    12.2. Īstenotie tehniskie un organizatoriskie aizsardzības pasākumi un šo pasākumu piemērotība personas datiem, kurus skāris Pārkāpums, jo īpaši tādi pasākumi, kas padara datus nesaprotamus personām, kurām nav pilnvaru piekļūt datiem, piemēram, šifrēšana;
    12.3. Turpmāk veiktie pasākumi un to spēja nodrošināt, lai nematerializētos augstais risks attiecībā uz Datu subjekta tiesībām un brīvībām;
    12.4. Paziņošanas Datu subjektam tehniskās iespējas.
13. Paziņošana Datu valsts inspekcijai tiek veikta aizpildot un iesniedzot veidlapu, kas ir šī dokumenta pielikums, kā arī atrodama Datu valsts inspekcijas mājas lapā www.dvi.gov.lv
14. Paziņošana Datu subjektam tiek veikta, izmantojot skaidru un vienkāršu valodu, iesniedzot paziņojumu vai gadījumā, ja tas prasītu nesamērīgi lielas pūles izmantojot publisku saziņu vai līdzīgu pasākumu, sniedz sekojošu informāciju:
    14.1. Pārkāpuma rakstura apraksts;
    14.2. Datu aizsardzības speciālista vārds, uzvārds un kontaktinformācija vai cits kontaktpunkts, kur var iegūt informāciju;
    14.3. Pasākumi, kas veikti, lai novērstu Pārkāpumu, un mazinātu tā iespējamās nelabvēlīgās sekas;
    14.4. Pārkāpuma iespējamās sekas.

Pielikumā:
1) Vadlīnijas datu aizsardzības pārkāpumu atklāšanai, novēršanai un paziņošanai
2) Paziņojuma Datu valsts inspekcijai veidlapa

Direktore D.Rozentāle

Pielikums Nr.1
pie Personas datu aizsardzības pārkāpumu atklāšanas, novēršanas un paziņošanas kārtības

Vadlīnijas
datu aizsardzības pārkāpumu atklāšanai, novēršanai un paziņošanai

Līdz ar Regulas spēkā stāšanos, stingrākai fizisko personu datu aizsardzībai, tiek ieviests pienākums personām, kas apstrādā personas datus (Pārziņiem) paziņot par Personas datu aizsardzības pārkāpumiem (Pārkāpums) Datu valsts inspekcijai, kā arī atsevišķos gadījumos indivīdiem, kuru tiesības ar šo pārkāpumu ir aizskartas. Šādam pienākumam ir vairāki mērķi un ieguvumi. Informējot Datu valsts inspekciju, par datiem atbildīgās personas, var iegūt informāciju par to, kā novērst pārkāpumu, vai Pārkāpuma smagums un raksturs ir tāds, lai pastāvētu par to pienākums ziņot skartajām personām un kā nodrošināt, lai šādi Pārkāpumi nenotiktu nākotnē. Pienākums ziņot personām savukārt nodrošina, ka fiziskās personas var saņemt informāciju par to kādi viņu personas dati ir tikuši ietekmēti un attiecīgi spert soļus, lai samazinātu pārkāpuma seku smagumu, piemēram, nomainīt paroles. **Pārkāpuma ziņošanas galvenais mērķis ir aizsargāt indivīdu tiesības šādu Pārkāpumu gadījumā.**

Kas ir pārkāpums?

Personas datu aizsardzības Pārkāpums Regulā tiek definēts, kā:

"drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, pazaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem" (turpmāk arī Pārkāpums)

Kā redzams definīcija ietver darbību uzskaitījumu, kas katra atsevišķi vai kopā uzskatāmas par Pārkāpumu. Datu "iznīcināšana" nozīmē, ka skartie dati vairs neeksistē vai neeksistē tādā formā, ka tie ir izmantojami. Datu "pazaudēšana" nozīmē, ka dati var vēl pastāvēt (nav zināms vai tie iznīcināti), bet Pārzinim vairs nav kontroles pār tiem, nav tiem pieejas, vai dati vairs nav Pārziņa rīcībā. "Datu pārveidošana" un "neatļauta izpaušana" arī ir sevi paskaidrojoši vārdi. Datu "pārveidošana" nozīmē to, ka dati vairs nav pilnīgi, savukārt "izpaušana", šajā kontekstā, nozīmē, ka dati tiek nodoti (vai tiek nodrošināta piekļuve) personām, bez tiesiska pamata un iemesla.

Piemērs. Datu pazaudēšanas var ietvert, piemēram, gadījumu kad ierīce (usb atmiņas karte, telefons, cietais disks, dators utt.), kurā saglabāti personas dati tiek nozagta vai pazaudēta. Pazaudēšanas gadījuma piemērs būtu arī, ja vienīgais eksemplārs ar personas datiem tiktu šifrēts datorvīrusa ietekmē vai arī, ja šādu eksemplāru kāds no darbiniekiem būtu šifrējis un aizmirstu vai pazaudētu piekļuves datus (paroli, atslēgu utt.)

Iespējams radīsies jautājums vai pagaidu traucējumi, piemēram, nespēja piekļūt kādai Pārziņa uzturētai datu bāzei vienu stundu, varētu tikt uzskatīts par Pārkāpumu, kā arī vai šāds notikums būtu jāpaziņo Datu valsts inspekcijai. Atbilstoši Regulai arī šādi pagaidu traucējumi piekļuvei datiem uzskatāmi par Pārkāpumiem (neattiecas uz plānotām sistēmas pārbaudēm, uzlabošanām utt.), jo šādi piekļuves traucējumi arī var atstāt iespaidu uz fizisku personu tiesībām un brīvībām. Tādēļ arī tie, demonstrējot Pārziņa atbildību pār datiem, būtu dokumentējami saskaņā ar šiem noteikumiem. Neskatoties uz dokumentēšanas pienākumu, Pārzinim var rasties un var nerasties pienākums ziņot par šo Pārkāpumu, ziņošanas pienākums izvērtējams katrā gadījumā individuāli.

Tāpat gadījumā, ja pieejamība ir traucēta tikai neilgu brīdi un nav atstājusi ietekmi uz fiziskām personām, ir svarīgi, lai Pārzinis izvērtētu arī citas iespējamās sekas šādam Pārkāpumam, ka jo šāds Pārkāpums var radīt citas, smagākas, sekas un var novest arī pie citiem Pārkāpumiem.

Piemērs. Datubāze ir inficēta ar ļaunatūru, kas šifrē datubāzi un pieprasa samaksu par datubāzes atbloķēšanu (ransomware), šāds Pārkāpums ietekmē datu pieejamību tikai īsu brīdi, gadījumā, ja datubāzi iespējams atjaunot no rezerves kopijas, tomēr, tīkla uzbrukums ir noticis un Pārzinim būtu pienākums rūpīgi izmeklēt šādu gadījumu. Paziņošana būtu nepieciešama, ja pārbaudes rezultātā atklātos, ka uzbrucējs būtu piekļuvis personas datiem.

Kādi ir biežākie Pārkāpumi?

Biežākie pārkāpumi, kā piemēri, var kalpot ātrākai un efektīvākai pārkāpuma atklāšanai un šādu pārkāpumu novēršanai, jo personas, apzinoties iespējamo pārkāpumu riskus, var no tā apzināti var izvairīties. Pie biežākajiem pārkāpumiem varētu pieskaitīt:

- Nozagta vai nozaudēta ierīce, kas satur personas datus;
- Dokuments ir nozaudēts vai atstāts brīvi pieejamā vietā;
- Pasts (papīra formā) ir nozaudēts vai piegādāts jau atvērts;
- Urķēšana, ļaunprogramatūra, pikšķērēšana;
- Nepareiza datu iznīcināšana;
- Nepārdomāta publikācija;
- Izpausti dati nepareizam datu subjektam;
- Personas dati nosūtīti nepareizam adresātam;
- Verbāla nesankcionēta datu izpaušana

Kādi ir pārkāpumu veidi?

Pārkāpumi tiek iedalīti pēc datu aizsardzības principiem, kurus Pārkāpumi ietekmē. Atbilstoši tie tiek iedalīti trīs sekojošās grupās.

- Konfidencialitātes pārkāpums. Šo pārkāpumu veidu raksturo nelikumīga vai nepamatota pieeja personas datiem. Kā, piemēram, tiek izpausti vairāk personas dati kā nepieciešams konkrētā mērķa sasniegšanai vai arī izpausti vairāk dati nekā piekritis datu subjekts;
- Integritātes pārkāpums. Integritātes pārkāpums ir tāds pārkāpums kā rezultātā dati apzināti vai nejauši tiek nelikumīgi izmainīti. Piemēram, dokumentā tiek ierakstīts nepareizs personas kods un cita cilvēka atzīmes;
- Pieejamības pārkāpums – apzināta vai nepazināta nepamatota piekļuves ierobežošana vai datu iznīcināšana. Piemēram, darba laikā, neplānoti, nav pieejamas nepieciešamās datu bāzes, studentam nepamatoti netiek vai tiek izsniegta tam nepieciešamā izziņa.

Jāatzīmē, ka viens un tas pats Pārkāpums var pārkāpt gan datu konfidencialitāti, gan integritāti, gan pieejamību vai jebkuru šo veidu kombināciju. Pārkāpums vienmēr it klasificējams kā pieejamības pārkāpums, ja dati ir tikuši nozaudēti vai iznīcināti.

Kad Pārzinim "kļūst zināms" par pārkāpumu?

Regula pieprasa, lai Pārkāpuma gadījumā, Pārzinis ziņot uzraugošajai iestādei (Datu valsts inspekcijai) bez nepamatotas kavēšanās un, ja iespējams, ne vēlāk kā 72 stundu laikā no brīža kad pārkāpums "kļuvis zināms". Šāds formulējums var radīt jautājumus, ko nozīmē "kļuvis zināms"? Būtu uzskatāms, ka pārzinim "kļuvis zināms" par pārkāpumu brīdī, kad Pārzinim ir saprātīgs pamats ticēt, ka ir noticis drošības incidents, kas ir novedis pie datu aizsardzības Pārkāpuma.

Regula pieprasa, lai Pārzinis īstenotu visus attiecīgos tehniskos un organizatoriskos pasākumus, lai nekavējoties konstatētu vai ir noticis personas datu aizsardzības pārkāpums, un ātri informētu uzraudzības iestādi un datu subjektu. Tieši šī iemesla dēļ izstrādāti šie noteikumi un vadlīnijas. Regula paskaidro, ka nosakot vai paziņojums veikts bez pamatotas kavēšanās, būtu jāņem vērā Pārkāpuma raksturu un smagumu, kā arī tā sekas un nelabvēlīgo ietekmi uz datu subjektu. Šis uzliek par pienākumu Pārzinim nodrošināt ka tam "kļūst zināms" katrs Pārkāpums bez nepamatotas kavēšanās, lai tas par to varētu ziņot noteiktajā

terminā. Kas nozīmē, ka ir svarīgi ne tikai kad pārkāpums "kļuvis zināms", bet ņemams arī vērā kad tam vajadzēja kļūt zināmam.

Precīzs brīdis, kad Pārzinim "kļūst zināms" par konkrētu Pārkāpumu ir atkarīgs no paša Pārkāpuma rakstura. Atsevišķos gadījums, noskaidrojot apstākļus, būs skaidrs, ka noticis Pārkāpums, tomēr, var būt gadījumi, kad nepieciešams laiks, lai noskaidrotu vai Pārkāpums tiešām noticis. Būtu nepieciešams likt uzsvaru uz nekavējošu darbību, lai izmeklētu incidentu un noskaidrotu vai personas dati ir tikuši skarti, un ja tā ir noticis, veikt darbības šo Pārkāpumu novēršanai un paziņot Datu valsts inspekcijai, ja nepieciešams.

Piemērs. Gadījumā, ja tikusi pazaudēta USB zibatmiņa (vai kāda cita ierīce) ar nešifrētiem personas datiem, bieži nav iespējams droši pateikt, ka šai informācijai piekļuvušas kādas trešās personas. Neskatoties uz to, ka šādu faktu nav iespējams konstatēt, par šādu faktu būtu jāinformē, jo ar saprātīgu ticamību iespējams konstatēt, ka personas datu drošība ir tikusi pārkāpta. Šajā gadījumā pārzinim "kļūst zināms" par Pārkāpumu brīdī, kad tiek konstatēts, ka ierīce ir pazudusi.

Piemērs. Trešā persona informē Pārzini, ka viņa nejauši saņēmusi datus par studenta atzīmēm un sniedz pierādījumus, ka šāds incidents tiešām ir noticis. Šādā gadījumā, ņemot vērā pierādījumus par Pārkāpumi, nav šaubu, ka Pārzinim ir "kļuvis zināms".

Piemērs. Pārzinis konstatē, ka tā tīklā, iespējams, ir notikusi ielaušanās. Pārzinis nekavējoties pārbauda tīkla sistēmas, lai noskaidrotu vai personu dati, kas tiek glabāti šajās sistēmās ir tikuši skarti un konstatē, ka šādā piekļuve ir bijusi iespējama. Šādā gadījumā Pārzinim ir pierādījumi, ka Pārkāpums ir noticis, līdz ar to, nevar būt šaubas, ka tam tas ir "kļuvis zināms".

Piemērs. Kibernoziedzinieks sazinās ar Pārzini un informē, ka sistēmā notikusi ielaušanās, lai prasītu izpirkuma maksu. Šādā gadījumā, Pārzinim pārbaudot sistēmu ir jāpārliecinās vai šāda ielaušanās ir notikusi, gadījumā, ja tas apstiprinās, nav šaubu, ka tam ir "kļuvis zināms".

Kā izriet no pēdējā piemēra, gadījumā, ja Pārzini par pārkāpumu informē kāda persona, medijs vai darbinieks, Pārzinis īsā periodā var veikt pārbaudi, lai noskaidrotu vai tiešām Pārkāpums ir noticis, t.i. apstiprināt ziņu patiesumu. Šajā īsajā periodā Pārzinis netiek uzskatīts par tādu kuram "kļuvis zināms". Neskatoties uz minēto ir sagaidāms, ka sākotnējā izmeklēšana būtu jāuzsāk pēc iespējas ātrāk un tajā būtu jānoskaidro vai pastāv saprātīga ticamība, ka incidents ir noticis; dziļāka izmeklēšana var notikt vēlāk.

Piemērs. Klients informē Pārzini, ka ir saņēmis e-pastu, kurā kāds izliekoties par Pārzini ir izmantojis klienta datus, kas saistīti ar Pārziņa patiesi sniegtajiem pakalpojumiem. Pārzinim vajadzētu veikt īsu izmeklēšanu, lai noskaidrotu vai tiešām notikusi ielaušanās tā sistēmās, gadījumā, ja šīs ziņas apstiprināts Pārzinis ir uzskatāms par tādu kuram "kļuvis zināms"

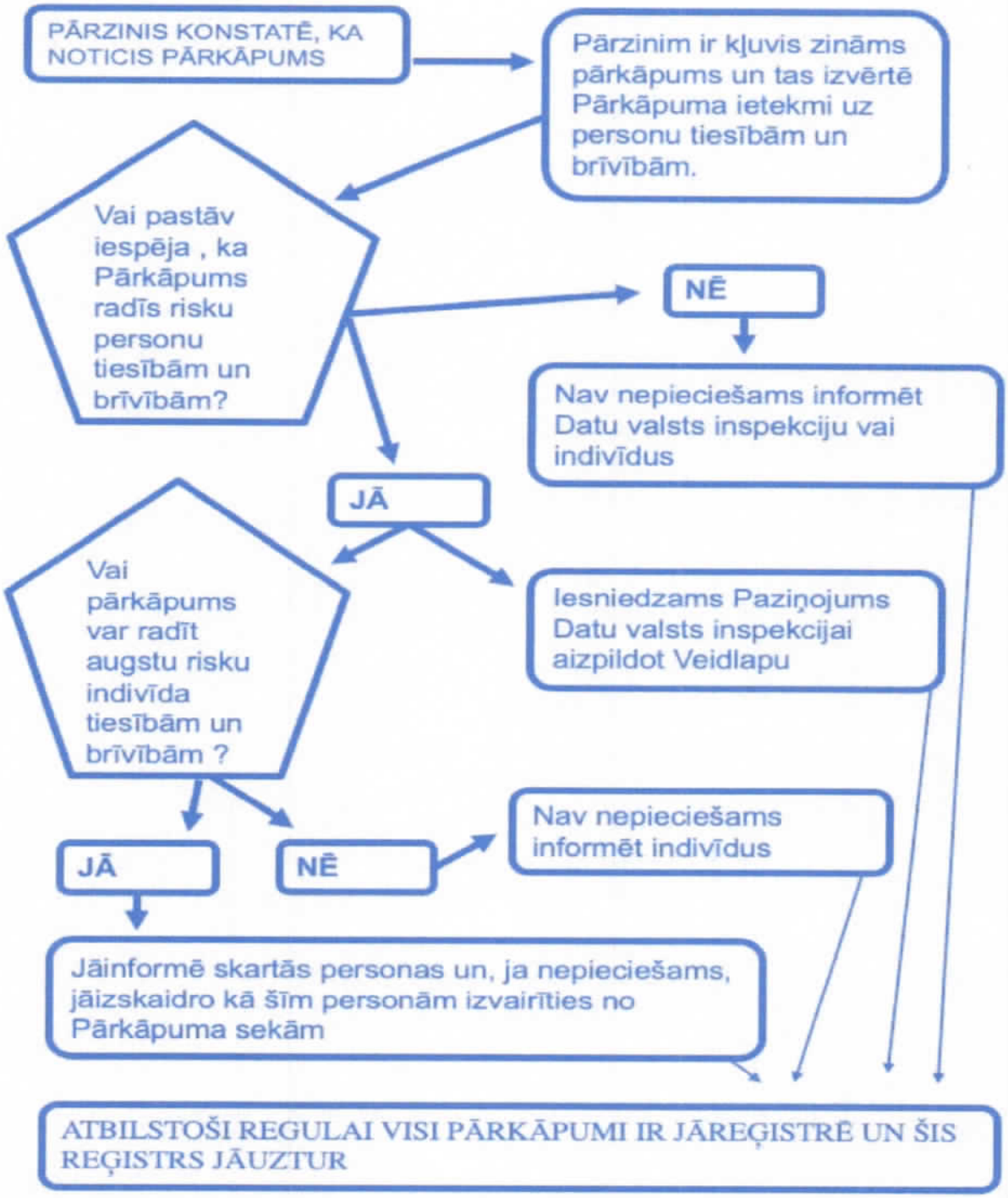
Kas ir Notikumu reģistrs?

Neatkarīgi no fakta vai Pārkāpums ir paziņojams Datu valsts inspekcijai Pārzinim ir pienākums ir uzturēt dokumentu, kurā tiek reģistrēti visi Pārkāpumi. Šis pienākums ir saistīts ar atbildības principu, kas nostiprināts Regulā. Tāpat paziņošanas ietvaros Datu valsts inspekcija var pieprasīt iepazīties ar šo Pārkāpumu, jeb Notikumu reģistru. Regula nenosaka stingru kārtību kādā vedams reģistrs, tomēr, būtu rekomendējams, ka katrā gadījumā, reģistrs iekļautu vismaz sekojošu informāciju a)Pārkāpuma veids un apraksts; b) Pārkāpuma sekas; c) Pārkāpuma rezultātā skartie personas dati d)Veiktās darbības Pārkāpuma un tā seku novēršanai. Tāpat būtu ieteicams pārzinim dokumentēt saistībā ar Pārkāpumu pieņemto lēmumu pamatotību, kā, piemēram, iekļaut pamatojumu kādēļ pieņemts lēmums par Pārkāpumu neziņot Datu valsts inspekcijai, ietverot, apsvērumus par Pārkāpuma ietekmi uz datu subjekta tiesībām un brīvībām.

Gadījumā, ja Paziņojums Datu valsts inspekcijai tiek iesniegts ar nokavēšanos, Pārzinim ir jāspēj pamatot šādas nokavēšanās iemeslus. Šādā gadījumā Reģistrs var palīdzēt pamatot nokavēšanās iemeslus.

Regula nenosaka cik ilgi šāds reģistrs būtu glabājams, ja Reģistrs satur personas datus, tad Pārzinim būtu jānosaka glabāšanas periods saskaņā ar likumīgas datu apstrādes principiem.

Kāda ir rīcības shēma Pārkāpuma gadījumā ?



**Papildus informācija par datu aizsardzības pārkāpumiem, to paziņošanas kārtību un fiksēšanas laiku u.c. jautājumiem pieejama angļu valodā vietnē www.ec.europa.eu (precīza saite www.ej.uz/fixy)*

Datu valsts inspekcija

Paziņojums par personas datu aizsardzības pārkāpumu

Dokumenta numurs (jāaizpilda tikai, ja šis ir papildus iesniegums)	
Iesnieguma veids	Sākotnējais iesniegums

1. Informācija par pārzini

1.1 Kontaktinformācija

Organizācijas nosaukums	
PVN reģistrācijas numurs	
Pasta adrese	*
Iesniedzējs	☐ pilnvarotā persona ☐ paraksttiesīgā persona * Jānorāda vai iesniedzējs ir pilnvarotā vai paraksttiesīgā persona
Iesniedzējs (vārds uzvārds)	*
Atbildīgā kontaktpersona (vārds uzvārds)	*
Atbildīgās personas amats	*
Elektroniskā pasta adrese	*
Tālruņa numurs	*

2. Laika grafiks

Pārkāpuma konstatēšanas datums	*
iemesls novēlotai paziņošanai par datu pārkāpumu	

3. Informācija par pārkāpumu * (obligāts vismaz viens no sekojošajiem variantiem)

Konfidencialitāte (nesankcionēta izpaušana vai nesankcionēta piekļuve) ☐

Integritāte (notikušas izmaiņas) ☐

Pieejamība (dati ir zaudēti vai iznīcināti) ☐

Pārkāpuma raksturs * (obligāts vismaz viens no sekojošajiem variantiem)

- ierīce ir nozaudēta vai nozagta ☐
- dokuments ir nozaudēts vai atstāts brīvi pieejamā vietā; ☐
- pasts (papīra firmātā) ir nozaudēts vai piegādāts atvērts; ☐
- urķēšana; ☐
- ļaunprogrammatūra (piem. ransomwares); ☐
- pikšķerēšana ; ☐
- nepareiza personas datu iznīcināšana papīra formātā; ☐
- E-atkritumi (personas dati atrodas novecojušā ierīcē); ☐
- nepārdomāta publikācija; ☐
- izpausti personas dati citam/nepareizam datu subjektam; ☐
- personas dati nosūtīti nepareizam adresātam; ☐
- verbāla nesankcionēta personas datu izpaušana ☐
- cits ☐

[Cits pārkāpuma raksturs] (nav jānorāda) ☐

Pārkāpuma cēlonis * (obligāts vismaz viens no sekojošajiem variantiem)

- Iekšēja neapzināta ļaunprātīga rīcība (iekšējās politikas pārkāpums) ☐
- iekšēja ļaunprātīga rīcība ☐
- ārēja neļaunprātīga rīcība ☐

ārējā Jaunprātīga rīcība ☐
Cits ☐

[Cits] pārkāpuma cēlonis (nav jānorāda) _____

4. Par apdraudēto datu kategorijām

Aptuvenais personas datu ierakstu skaits, kurus skar pārkāpums _____ *

* (obligāts vismaz viens no sekojošajiem variantiem)

4.1 Vispārējie dati

Datu subjekta identitāte (vārds, uzvārds, dzimšanas datums) ☐
Nacionālais identifikācijas numurs ☐
Kontaktinformācija ☐
Identificējoši dati ☐
Ekonomiskie un finanšu dati ☐
Oficiālie dokumenti ☐
Atrašanās vietas dati ☐
Informācija par kriminālsodāmību un/vai nodarījumiem, vai uzliktajiem drošības pasākumiem ☐

4.2 Īpašās datu kategorijas

Dati, kas atklāj rasi vai etnisko piederību ☐
Politiskie uzskati ☐
Reliģiskie vai filozofiskie uzskati ☐
Dalība arodbiedrībā ☐
Dati par seksuālo dzīvi ☐
Veselības dati ☐
Ģenētiskie dati ☐
Biometriskie dati ☐
Nav vēl zināms ☐

Cits ☐

'Cits' apraksts (nav jānorāda) _____

5. Informācija par datu subjektiem

* (obligāts vismaz viens no sekojošajiem variantiem)

- Nodarbinātie ☐
- Lietotāji ☐
- Abonētāji ☐
- Studenti ☐
- Militārais personāls ☐
- Klients (pašreizējie un potenciālie) ☐
- Pacienti ☐
- Nepilngadīgie ☐
- Neaizsargātas personas ☐
- Vēl nav zināms ☐
- Cits ☐

'Cits' apraksts (nav jānorāda)

detalizēts iesaistīto datu subjektu apraksts

aptuvenais personu skaits, uz kurām attiecas pārkāpums

6. Par pasākumiem, kas ieviesti pirms pārkāpuma

7. Sekas

* (obligāts vismaz viens no sekojošajiem variantiem)

7.1 Konfidencialitātes pārkāpums

- Plašāka izpaušana, kā nepieciešama mērķa sasniegšanai, vai kādai piekrituši datu subjekti ☐
- Apstrādātie dati var būt saistīti ar datu subjekta citu informāciju ☐

Dati var tikt izmantoti citiem mērķiem un/vai negodprātīgā veidā	☐
Cits	☐
'Cits' konfidencialitātes pārkāpuma seku apraksts (nav jānorāda)	

7.2 Integritātes pārkāpums

Dati ir/var būt modificēti un tiek izmantoti, kaut arī tie vairs nav derīgi	☐
Dati ir/var būt modificēti citos derīgos datos un izmantoti citiem mērķiem	☐
Cits	☐
'Cits' integritātes pārkāpuma seku apraksts (nav jānorāda)	

7.3 Pieejamības pārkāpums

būtiska pakalpojuma sniegšanas iespējas zudums ietekmētajiem datu subjektiem	☐
būtiska pakalpojuma sniegšanas iespējas maiņa ietekmētajiem datu subjektiem	☐
Cits	☐
'Cits' pieejamības pārkāpuma seku apraksts (nav jānorāda)	

7.4 Fiziski, materiāli vai nemateriāli kaitējums vai būtiskas sekas datu subjektiem

Potenciālās ietekmes uz datu subjektu apraksts

zaudēta kontrole pār saviem personas datiem;	☐
ierobežotas personas tiesības;	☐
diskriminācija;	☐
identitātes zādzība;	☐
krāpšana;	☐
finansiālais zaudējums;	☐

neatļauta pseidonimizācijas atcelšana; ☐
kaitējums reputācijai; ☐
personas datu, ko aizsargā dienesta noslēpums, konfidencialitātes zaudēšana; ☐
Cits ☐

'Cits' potenciālās ietekmes uz datu subjektu apraksts (nav jānorāda)

Iespējamo datu pārkāpuma ietekmes seku datu subjektam novērtējums

* (obligāti jāizvēlas tikai viens no sekojošajiem variantiem)

nenozīmīgs ☐
maznozīmīgs ☐
nozīmīgs ☐
ļoti nozīmīgs ☐

8. Veicamās darbības

8.1 Paziņošana datu subjektiem

Datu subjekta informēšana:

* (obligāti jāizvēlas tikai viens no sekojošajiem variantiem)

Jā ☐
Nē, bet tiks informēts ☐
Nē, netiks informēti ☐
Nav zināms ☐

(nav jānorāda) ☐

Iemesls kāpēc datu subjekts netiks informēts par datu pārkāpumu:

Sekojošā informācija nav jānorāda

Kontrolieris ir ieviesis atbilstošus tehniskos un organizātoriskās prasības un piemērojis personas datu pārkāpuma skartajiem personas datiem, it īpaši tiem, kuri ir neaizsargāti, brīvi pieejami citām neautorizētām personām ☐

Kontrolieris ir veicis atbilstošas darbības, kas ☐

nodrošina, ka datu subjekta tiesības un brīvība turpmāk nematerializēsies;
Tas ietvertu nesamērīgus pūliņus, lai katru datu subjektu informētu individuāli

Informācija nav nepieciešama

Datu subjektam sniegtās informācijas saturs pievienots pielikumā

Informācija nav nepieciešama

8.2 Pārziņa veiktie pasākumi pārkāpuma ietekmes mazināšanai

Apraksta pasākumus, ko pārzinis veicis, lai mazinātu pārkāpuma ietekmi *

8.3 Pārrobežu un citi paziņojumi

Vai šis paziņojums ir sagatavots kā pārrobežu paziņojums, kas nosūtīts vadošajai uzraudzības iestādei?

ES valstu saraksts, uz kurām attiecas datu pārkāpums (jānorāda valsts kods; piemērs: EN, FR, ...)