SMILTENES NOVADA DOME

Reģ. Nr. 90009067337, Dārza iela 3, Smiltene, Smiltenes novads, LV-4729
tālr.: 64774844, fakss: 64707583, e-pasts: dome@smiltene.lv

LĒMUMS
Smiltenē

2019.gada 27.februārī Nr. 184
(protokols Nr.2, 20.§.)

Noteikumu Nr.4/19 "Personas datu aizsardzības pārkāpumu atklāšanas, novēršanas un paziņošanas kārtība" apstiprināšana

Dome izskata personas datu aizsardzības speciālista izstrādāto noteikumu "Personas datu aizsardzības pārkāpumu atklāšanas, novēršanas un paziņošanas kārtība" projektu (turpmāk - Noteikumi). Noteikumi nosaka personas datu aizsardzības pārkāpumu atklāšanas, novēršanas un paziņošanas kārtība" nosaka vienotu kārtību, kādā domē un tās iestādēs tiek veiktas darbības, lai atklātu, novērstu un reģistrētu personas datu aizsardzības pārkāpumus un normatīvajos aktos noteiktajos gadījumos veiktu paziņošanu par konstatētajiem pārkāpumiem Datu subjektam un/vai Datu valsts inspekcijai, kā arī novērstu šo pārkāpumu radītās nelabvēlīgās sekas.

Atbilstoši Eiropas Parlamenta un Padomes 2016.gada 27.aprīļa regulas (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 33. pantam personas datu aizsardzības pārkāpuma gadījumā pārzinis bez nepamatotas kavēšanās un, ja iespējams, ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tam kļuvis zināms, paziņo par personas datu aizsardzības pārkāpumu uzraudzības iestādei. Ja paziņošana uzraudzības iestādei nav notikusi 72 stundu laikā, paziņojumam pievieno kavēšanās iemeslus.

Noteikumi ir pašvaldības iekšējie noteikumi un ir spēkā attiecībā uz visām pašvaldības amatpersonām un darbiniekiem.

Vadoties no iepriekšminēta, Finanšu un attīstības jautājumu pastāvīgās komitejas 2019.gada 19.februāra atzinumu (sēdes protokols Nr.2) un pamatojoties uz Izdots saskaņā ar Valsts pārvaldes iekārtas likuma 72.panta pirmās daļas 2.punktu, 73.panta pirmās daļas 4.punktu un likuma "Par pašvaldībām" 41.panta 2.punktu, atklāti balsojot ar 13 balsīm par (Gints Kukainis, Aigars Dudelis, Aija Cunska, Aigars Veldre, Ināra Grundāne, Edgars Avotiņš, Birute Mežale, Vairis Tralla, Kaspars Markss, Ilze Vergina, Tija Zaļkalne, Andis Rozītis, Kārlis Lapiņš), pret – nav, atturas – nav,
Smiltenes novada dome
NOLEMJ:

1. Apstiprināt noteikumus Nr.4/19 "Personas datu aizsardzības pārkāpumu atklāšanas, novēršanas un paziņošanas kārtība" (pielikumā).
2. Noteikumu izpildi kontrolēt izpilddirektoram.
3. Lēmums stājas spēkā ar tā pieņemšanas dienu.

Domes priekšsēdētājs G.Kukainis

SMILTENES NOVADA DOME

Reģ. Nr. 90009067337, Dārza iela 3, Smiltene, Smiltenes novads, LV-4729
tālr.: 64774844, fakss: 64707583, e-pasts: dome@smiltene.lv

NOTEIKUMI
Smiltenē

2019. gada 27.februārī Nr. 4/19

Apstiprināti
ar Smiltenes novada domes
2019. gada 27. februāra lēmumu Nr. 184
(sēdes protokols Nr.2, 20.§)

Personas datu aizsardzības pārkāpumu atklāšanas, novēršanas un paziņošanas kārtība

Izdots saskaņā ar Valsts pārvaldes iekārtas likuma 72.panta pirmās daļas 2.punktu, 73.panta pirmās daļas 4.punktu un likuma "Par pašvaldībām" 41.panta 2.punktu

I. Vispārīgie noteikumi

1. Noteikumi "Personas datu aizsardzības pārkāpumu atklāšanas, novēršanas un paziņošanas kārtība" nosaka vienotu kārtību, kādā Pašvaldībā un tās iestādēs tiek veiktas darbības, lai atklātu, novērstu un reģistrētu personas datu aizsardzības pārkāpumus un normatīvajos aktos noteiktajos gadījumos veiktu paziņošanu par konstatētajiem pārkāpumiem Datu subjektam un/vai Datu valsts inspekcijai, kā arī novērstu šo pārkāpumu radītās nelabvēlīgās sekas.
2. Noteikumos ir lietoti šādi termini un saīsinājumi:
2.1. Noteikumi – šie Smiltenes novada pašvaldības personas datu aizsardzības pārkāpumu atklāšanas, novēršanas un paziņošanas kārtība;
2.2. Pašvaldība – Smiltenes novada dome un tās izveidotās institūcijas un iestādes;
2.3. Pārkāpums – personas datu aizsardzības pārkāpums, kura rezultātā ar nodomu (tīši) vai aiz neuzmanības notiek Pašvaldības pārziņā esošo personas datu nozaudēšana, neatļauta iznīcināšana, pārveidošana, izpaušana, piekļuves nodrošināšana tiem vai ir tikusi ietekmēta to integritāte vai pieejamība tiem;
2.4. Nodarbinātie – Pašvaldības amatpersonas un darbinieki;
2.5. Speciālists – Pašvaldības personas datu aizsardzības speciālists;
2.6. 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;
2.7. Reģistrs – notikumu reģistrs, kurā tiek reģistrēti visi Pārkāpumi.
Termini, kas nav definēti šajā punktā, tiek izmantoti atbilstoši to Regulā ietvertajai nozīmei.
3. 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.

II. Darbinieku pienākumi un rīcība pārkāpumu gadījumā

4. Visiem darbiniekiem ir pienākums iepazīties ar šo Kārtību, zināt raksturīgākos Pārkāpumu veidus (1. pielikums), veikt savas kompetences un iespēju robežās visas nepieciešamās darbības, lai novērstu un/vai pārtrauktu Pārkāpumus, novērstu vai mazinātu Pārkāpuma nelabvēlīgās sekas, kā arī nekavējoties ziņot par Pārkāpumu Speciālistam.

5. Darbinieks, konstatējot Pārkāpumu, nekavējoties, bet ne vēlāk kā 8 stundu laikā, ziņo Speciālistam, e-pasta sūtījumā norādot informāciju par Pārkāpumu, Pārkāpuma sekām, kā arī informāciju par darbībām, kas ir veiktas Pārkāpuma novēršanai, pārtraukšanai, Pārkāpuma seku novēršanai vai mazināšanai.
6. Darbiniekiem ir pienākums ziņot par konstatētajiem 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; Pašvaldības apstrādātājiem (sadarbības partneriem); saņemot publiski pieejamu informāciju; veicot Pašvaldībā pārbaudi vai auditu.

7. 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. SPECIĀLISTA PIENĀKUMI UN RĪCĪBA PĀRKĀPUMA GADĪJUMOS, PĀRKĀPUMU PAZIŅOŠANA

8. Speciālists:
   8.1. veic Pārkāpuma novēršanu, apturēšanu, seku novēršanu vai mazināšanu;
   8.2. uztur Reģistru un veic tajā informācijas papildināšanu/atjaunināšanu;
   8.3. nepieciešamības gadījumā, nodrošina paziņošanu par Pārkāpumiem Datu valsts inspekcijai;
   8.4. veic citus Kārtībā un spēkā esošajos normatīvajos aktos noteiktos pienākumus.
9. Pēc informācijas par iespējamo Pārkāpumu saņemšanas Speciālists Pārkāpumu tajā pašā dienā reģistrē Reģistrā.
10. Speciālists nekavējoties veic darbības, lai Pārkāpums tiktu novērsts vai pārtraukts un tiktu novērstas vai mazinātas Pārkāpuma nelabvēlīgās sekas (ja šādas darbības jau nav veicis darbinieks, kurš ziņoja par Pārkāpumu).
11. Speciālists izvērtē, vai Pārkāpums var radīt risku datu subjekta tiesībām un brīvībām. Ja Speciālists konstatē, ka pastāv varbūtība, ka Pārkāpums var radīt risku datu subjektu tiesībām un brīvībām, tad Speciālists rakstveidā dokumentē savu slēdzienu, un iesniedz to Pašvaldības izpilddirektoram.
12. Pašvaldības izpilddirektors pēc Kārtības 11.punktā minētā atzinuma saņemšanas nekavējoties to izskata. Ja Pašvaldības izpilddirektors atzīst, ka Speciālista atzinums ir pamatots, tad Pašvaldības izpilddirektors pieņem lēmumu par Pārkāpuma paziņošanu Datu subjektam un/vai Datu valsts inspekcijai, un uzdod to nodrošināt Speciālistam vai citai personai.
13. Speciālists, pieņemot slēdzienu (11.punkts) un Pašvaldības izpilddirektors pieņemot galīgo lēmumu, jo īpaši ņem vērā šādus apstākļus:
   13.1. pārkāpuma radītais risks fizisku personu tiesībām un brīvībām;
   13.2. 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;
   13.3. turpmāk veiktie pasākumi un to spēja nodrošināt, lai nematerializētos augstais risks attiecībā uz Datu subjekta tiesībām un brīvībām;
   13.4. paziņošanas Datu subjektam tehniskās iespējas.
14. Paziņošana Datu valsts inspekcijai tiek veikta, iesniedzot paziņojumu – Datu valsts inspekcijas mājaslapā publicēto speciālo veidlapu, kurā ir ietverta šāda informācija:
   14.1. pārkāpuma raksturs, ietekmēto datu subjektu kategorijas un datu subjektu aptuvenais skaits, ietekmētie personas datu veidi un datu apjoms;
   14.2. pārkāpuma iespējamās nelabvēlīgās sekas;
   14.3. pasākumi, ko Pašvaldība veikusi, lai novērstu Pārkāpumu, un mazinātu tā iespējamās nelabvēlīgās sekas;
   14.4. gadījumā, ja paziņošana Datu valsts inspekcijai notiek vēlāk nekā 72 stundu laikā no Pārkāpuma konstatēšanas brīža, paziņojumam pievieno kavēšanās iemeslus.
   14.5. speciālista vārds, uzvārds un kontaktinformācija vai cita kontaktpersona, no kuras var iegūt informāciju.

15. 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:
    15.1. pārkāpuma iespējamās nelabvēlīgās sekas;
    15.2. pasākumi, ko Pašvaldība veikusi, lai novērstu Pārkāpumu, un mazinātu tā iespējamās nelabvēlīgās sekas;
    15.3. pasākumi, kurus vēlams veikt Datu subjektam, lai mazinātu Pārkāpuma iespējamās nelabvēlīgās sekas;
    15.4. speciālista vārds, uzvārds un kontaktinformācija vai cita kontaktpersona, no kuras var iegūt informāciju.

Domes priekšsēdētājs G.Kukainis

1. pielikums
2019.gada 27.februāra Noteikumiem Nr.4/19

Tipiskākie personas datu aizsardzības pārkāpumu veidi un piemēri pašvaldībās

Personas datu aizsardzības pārkāpumus parasti klasificē trīs veidos, kas var palīdzēt pārziņa atbildīgajam personālam (darbiniekiem) labāk orientēties dažādos pārkāpumu piemēros:

- Konfidencialitātes pārkāpums (visbiežākais pārkāpumu veids): atbildīgā persona (darbinieks) personas datus ievāc pretlikumīgi (ievākšana nav pieļaujama), izpauž pretlikumīgi (datiem piekļūst, tos izpauž vai nodod neautorizētai personai) vai apstrādā datus citā pretlikumīgā veidā.
- Integritātes pārkāpums: datus izmaina vai iznīcina neautorizēta persona.
- Pieejamības pārkāpums: rada fizisks vai tehnisks traucējums, kā rezultātā atbildīgajām personām (darbiniekiem) pazūd piekļuve personas datiem.

Veids	**Piemēri**	**Vieds**	**Piemēri**	**Veids**	**Piemēri**
Konfidencialitātes pārkāpumi	Uzzinot darbinieka pieejas paroli, jo tā nav pietiekami aizsargāta, cita persona piekļūst informācijas sistēmai un aplūko datus (izdara kopiju)	***Integritātes pārkāpumi***	Uzzinot darbinieka pieejas paroli, jo tā nav pietiekami aizsargāta, cita persona piekļūst informācijas sistēmai un izmaina tās datus	***Pieejamības pārkāpumi***	Elektrības pārrāvuma, kiberuzbrukuma vai citu tehnisku faktoru rezultātā zaudēta pieeja elektroniski glabātajiem personas datiem
	Personas datus saturoša e-pasta nosūtīšana nepareizajam adresātam				Dokumentu seifa atslēgas nozaudēšanas, ugunsgrēka vai citu fizisku faktoru rezultātā zaudēta pieeja papīra dokumentos glabātajiem personas datiem
	Personas datu atklāšana personai bez identitātes pārbaudes (piemēram, pa telefonu)				
	Personas datu nodošana kolēģu starpā, ja tas nav nepieciešams darba pienākumu veikšanai				
	Personas datus saturoša dokumenta nozaudēšana (arī zādzība) vai atstāšana bez uzraudzības klientiem/apmeklētājiem brīvi pieejamā vietā				
	IT drošības caurumu vai šaubīgu e-pastu rezultātā iekšējām informācijas sistēmām piekļūst ārējas personas				
	Darba portatīvā datora vai citas pārnēsājamas ierīces nozaudēšana – arī tad, ja datiem uz ierīces ir rezerves kopija				

2. pielikums
2019.gada 27.februāra Noteikumiem Nr.___19

DATU AIZSARDZĪBAS PĀRKĀPUMU UZSKAITES REĢISTRS

Datu pārziņa rekvizīti	
Nosaukums	Smiltenes novada pašvaldība
Adrese	Dārza iela 3, Smiltene, Smiltene novads, LV-4729
E-pasta adrese	dome@smiltene.lv
Tālruņa numurs	64 707 588

Nr.p.k.	ZIŅAS PAR PĀRKĀPUMU					Pārkāpuma notikušās vai iespējamās sekas datu subjektiem	ZIŅAS PAR PĀRKĀPUMA SEKU NOVĒRŠANAS VAI IEROBEŽOŠANAS PASĀKUMIEM		
	Pārkāpuma datums	Pārkāpuma kategorija	Pārkāpuma detalizēts apraksts	Personas datu kategoriju uzskaitījums, kurus ietekmēja pārkāpums	Pārkāpuma ietekmēto datu subjektu skaits (aptuvens)		Vai ir informēta Datu valsts inspekcija	Vai ir informēti datu subjekti	Īstenoto pasākumu apraksts
1.									
2.									
3.									
4.									
5.									
6.									
7.									
8.									
9.									
		Piemēri: darbinieka pārkāpums, IT sistēmu kļūda, apstrādātāja pārkāpums			Precīzs vai, ja nav iespējams noteikt - aptuvens skaits				

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, jeb 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 pacientu 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.

Piemērs. Ārstniecības iestādes kontekstā, ja būtiski medicīniskie dati nav pieejami, pat uz īsu brīdi, tas var novest pie pacienta tiesību un brīvību aizskāruma, piemēram, veselībai

svarīgas manipulācijas vai operācijas var tikt atliktas, jo nav pieejas svarīgai informācijai, tādējādi pat apdraudot šo personu dzīvību un veselību.

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 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 diagnoze;
- Pieejamības pārkāpums – apzināta vai nepazināta nepamatota piekļuves ierobežošana vai datu iznīcināšana. Piemēram, darba laikā, neplānoti, nav pieejamas nepieciešamās datu bāzes.

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. Tāpat 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 termiņā. 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 Pārziņa klientu 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"

**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/ftxy)*