*Novērtējums par ietekmi uz datu aizsardzību*

Saturs

[1. Tiesiskais regulējums 3](#_Toc516851110)

[1.1. Vispārīgā datu aizsardzības regula (VDAR) 3](#_Toc516851111)

[2. Kad nepieciešams NIDA? 5](#_Toc516851112)

[2.1. Pamati 5](#_Toc516851113)

[2.2. Gadījumi, kad NIDA veicams obligāti 6](#_Toc516851114)

[2.2.1. Papildus apsvērumi par nepieciešamību veikt NIDA 6](#_Toc516851115)

[2.2.2. NIDA veikšana vairāku līdzīgu apstrādes darbību kopumam 7](#_Toc516851116)

[2.2.3. Pozitīvie un negatīvie saraksti NIDA veikšanai 7](#_Toc516851117)

[2.3. Kad jāveic NIDA? 7](#_Toc516851118)

[2.4. NIDA pārskatīšana 8](#_Toc516851119)

[2.5. Apspriešanās ar datu uzraudzības iestādi saskaņā ar VDAR 36.pantu 8](#_Toc516851120)

[3. Kas ir atbildīgs par NIDA veikšanu? 9](#_Toc516851121)

[3.1. Pamati 9](#_Toc516851122)

[3.2. Piedalīšanās NIDA 9](#_Toc516851123)

[4. Kā veikt NIDA? 10](#_Toc516851124)

[4.1. Pamati 10](#_Toc516851125)

[4.2. NIDA īstenošana 10](#_Toc516851126)

[4.3. NIDA minimālais saturs 10](#_Toc516851127)

[4.4. NIDA process 11](#_Toc516851128)

[4.5. Datu subjektu vai to pārstāvju iekļaušana 13](#_Toc516851129)

[4.6. Ziņojums par NIDA 14](#_Toc516851130)

[5. Secinājumi un praktiski padomi 16](#_Toc516851131)

[6. Ārējie avoti un tīmekļa vietnes 17](#_Toc516851132)

[6.1. Grāmatas un publikācijas 17](#_Toc516851133)

[6.2. 29.panta darba grupas dokumenti 17](#_Toc516851134)

[6.3. Tīmekļa saites 17](#_Toc516851135)

# Tiesiskais regulējums

## Vispārīgā datu aizsardzības regula (VDAR)

*35.pants*

*Novērtējums par ietekmi uz datu aizsardzību*

*1. Ja apstrādes veids, jo īpaši, izmantojot jaunās tehnoloģijas un ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūkus, varētu radīt augstu risku fizisku personu tiesībām un brīvībām, pārzinis pirms apstrādes veic novērtējumu par to, kā plānotās apstrādes darbības ietekmēs personas datu aizsardzību. Vienā novērtējumā var pievērsties tādu līdzīgu apstrādes darbību kopumam, kurām piemīt līdzīgi augsti riski.*

*2. Pārzinis, veicot novērtējumu par ietekmi uz datu aizsardzību, lūdz padomu no datu aizsardzības speciālista, ja tāds ir iecelts.*

*3. Šā panta 1. punktā minētais novērtējums par ietekmi uz datu aizsardzību jo īpaši ir vajadzīgs šādos gadījumos:*

*a) ar fiziskām personām saistītu personisku aspektu sistemātiska un plaša novērtēšana, kuras pamatā ir automatizēta apstrāde, tostarp profilēšana, un ar kuru pamato lēmumus, kas fiziskai personai rada tiesiskās sekas vai līdzīgi būtiski ietekmē fizisko personu;*

*b) 9. panta 1. punktā minēto īpašo kategoriju datu vai 10. pantā minēto personas datu par sodāmību un pārkāpumiem apstrāde plašā mērogā; vai*

*c) publiski pieejamas zonas sistemātiska uzraudzība plašā mērogā.*

*4. Uzraudzības iestāde izstrādā un publisko sarakstu ar tiem apstrādes darbību veidiem, attiecībā uz kuriem ir jāveic novērtējums par ietekmi uz datu aizsardzību saskaņā ar 1. punktu. Uzraudzības iestāde minētos sarakstus iesniedz 68. pantā minētajai kolēģijai.*

*5. Uzraudzības iestāde var izstrādāt un publiskot arī sarakstu ar tiem apstrādes darbību veidiem, attiecībā uz kuriem nav vajadzīgs novērtējums par ietekmi uz datu aizsardzību. Uzraudzības iestāde minētos sarakstus iesniedz kolēģijai.*

*6. Ja 4. un 5. punktā paredzētais saraksts ietver apstrādes darbības, kas ir saistītas ar preču vai pakalpojumu sniegšanu datu subjektiem vai ar viņu uzvedības novērošanu vairākās dalībvalstīs, vai kas var būtiski ietekmēt personas datu brīvu apriti Savienībā,*

*kompetentā uzraudzības iestāde pirms minētā saraksta pieņemšanas piemēro 63. pantā paredzēto konsekvences mehānismu.*

*7. Novērtējumā ietver vismaz:*

*a) plānoto apstrādes darbību un apstrādes nolūku, tostarp attiecīgā gadījumā pārziņa leģitīmo interešu sistemātisku aprakstu;*

*b) novērtējumu par apstrādes darbību nepieciešamību un samērīgumu attiecībā uz nolūkiem;*

*c) novērtējumu par 1. punktā minētajiem riskiem datu subjektu tiesībām un brīvībām; un*

*d) pasākumus, kas paredzēti risku novēršanai, tostarp garantijas, drošības pasākumus un mehānismus, ar ko nodrošina personas datu aizsardzību un uzskatāmi parāda, ka ir ievērota šī regula, ņemot vērā datu subjektu un citu attiecīgo personu tiesības un leģitīmās intereses.*

*8. Attiecīgo pārziņu vai apstrādātāju atbilstību 40. pantā minētajam rīcības kodeksam pienācīgi ņem vērā, novērtējot šādu pārziņu vai apstrādātāju veikto apstrādes darbību ietekmi, jo īpaši saistībā ar novērtējumu par ietekmi uz datu aizsardzību.*

*9. Attiecīgā gadījumā pārzinis pieprasa datu subjektu vai viņu pārstāvju viedokli par plānoto apstrādi, neskarot komerciālu vai sabiedrības interešu aizsardzību vai apstrādes darbību drošību.*

*10. Ja saskaņā ar 6. panta 1. punkta c) vai e) apakšpunktu veiktās apstrādes juridiskais pamats ir noteikts Savienības tiesību aktos vai tās dalībvalsts tiesību aktos, kuri ir piemērojami pārzinim, un minētie tiesību akti reglamentē konkrēto apstrādes darbību vai minēto darbību kopumu, un novērtējums par ietekmi uz datu aizsardzību jau ir veikts kā daļa no vispārējā ietekmes novērtējuma saistībā ar minētā juridiskā pamata pieņemšanu, šā panta 1.–7. punktu nepiemēro, izņemot, ja dalībvalstis uzskata, ka pirms apstrādes darbībām ir jāveic šāds novērtējums.*

*11. Ja vajadzīgs, pārzinis veic pārskatu, lai novērtētu, vai apstrāde notiek saskaņā ar novērtējumu par ietekmi uz datu aizsardzību, vismaz tad, ja ir izmaiņas attiecībā uz apstrādes darbību radīto risku.*

*89. līdz 96. apsvērums.*

VDAR 35.pants ir cieši saistīts ar 24., 25. un 32.pantu. Galvenā atšķirība starp 32.pantu un 35.pantu ir tāda, ka 32.pants (Apstrādes drošība) ir vērsts uz riskiem, kas saistīti ar nelabvēlīgiem notikumiem, piemēram, uzbrukumiem, bet novērtējums par ietekmi uz datu aizsardzību (NIDA), kas balstīts uz 35.pantu, galvenokārt **koncentrējas uz riskiem, kas izriet no regulāras datu apstrādes.**

NIDA ir svarīgs instruments datu aizsardzības īstenošanā ar tehnoloģiskiem līdzekļiem (integrēta datu aizsardzība), kā noteikts 25.panta 1.punktā. Abi ir balstīti uz piesardzības principu, t.i., lai identificētu riskus agrīnās izstrādes posmos, lai pirms datu apstrādes sistēmu ieviešanas un to darbības uzsākšanas apsvērtu piemērotus pretpasākumus.

NIDA ir līdzeklis, lai identificētu un analizētu šādus riskus. Gadījumos, kad NIDA nav obligāts, saistīto risku analīze tomēr ir nepieciešama, lai pienācīgi īstenotu 25. un 32.panta prasības. Abi panti skaidri atsaucas uz fizisko personu tiesībām un brīvībām. Veicamās riska analīzes dziļums un nepieciešamā dokumentācija ir atkarīga no apstrādes sarežģītības un riska pakāpes. Mēs iesakām riska analīzes dokumentāciju nodrošināt rakstveidā.

Integrētas datu aizsardzības principa īstenošana sniedzas ārpus riskiem, kas iepriekš noteikti vispārējā riska analīzē, un tajā ietverti lēmumi, ko šim nolūkam sistēmas izstrādātāji (privātuma inženierija) ir pieņēmuši vēlākā stadijā, īstenojot datu minimizēšanas principus.

# Kad nepieciešams NIDA[[1]](#footnote-1)?

## Pamati

NIDA jāveic pirms tādas personas datu apstrādes, kas varētu apdraudēt fizisko personu tiesības un brīvības.

Principā NIDA ir jāveic jebkura veida datu apstrādei, ja vien *a priori* var noteikt, ka konkrētu datu apstrādes darbības neietekmēs fizisko personu tiesības un brīvības.

Par to, kāda veida datu apstrādei jānovērtē šādi riski izklāstīts, piemēram, 35.panta 3.punktā vai 91.apsvērumā. Šeit uzsvars tiek likts uz tā saucamo jauno tehnoloģiju izmantošanu (kas ir neskaidrs juridiskais jēdziens), kas ieviests VDAR attiecībā uz NIDA.

Riska novērtējumā jāņem vērā ne tikai pastāvošie riska scenāriji, bet arī nākotnes notikumu iespējamība, kas jāidentificē prognostiskā novērtējumā. Novērtējuma rezultāti ir jādokumentē.

35.panta 1.punkta pēdējais teikums kopā ar 92.apsvērumu sniedz svarīgu viedokli par NIDA nepieciešamības novērtēšanu: “Noteiktos apstākļos var būt saprātīgi un ekonomiski veikt plašāku novērtējumu par ietekmi uz datu aizsardzību, kura priekšmets nav tikai viens projekts, piemēram, ja publiskas iestādes vai struktūras vēlas izveidot vienotu lietotņu vai apstrādes platformu vai ja vairāki pārziņi plāno ieviest vienotu lietotņu vai apstrādes vidi kādā rūpniecības nozarē vai segmentā, vai kādai plaši lietotai horizontālai darbībai.”

## Gadījumi, kad NIDA veicams obligāti

35.panta 3.punktā uzskaitīti gadījumi, kad NIDA veicams obligāti:

1. *ar fiziskām personām saistītu personisku aspektu sistemātiska un plaša novērtēšana, kuras pamatā ir automatizēta apstrāde, tostarp profilēšana, un ar kuru pamato lēmumus, kas fiziskai personai rada tiesiskās sekas vai līdzīgi būtiski ietekmē fizisko personu;*
2. *9. panta 1. punktā minēto īpašo kategoriju datu vai 10. pantā minēto personas datu par sodāmību un pārkāpumiem apstrāde plašā mērogā; vai*
3. *publiski pieejamas zonas sistemātiska uzraudzība plašā mērogā.*

### Papildus apsvērumi par nepieciešamību veikt NIDA

91.apsvērumā uzskaitīti citi gadījumi, kad nepieciešams veikt NIDA:

Apstrādes darbības

a) kas potenciāli ietver lielu cilvēku skaitu un/vai augsta līmeņa risku un/vai plaša mēroga tehnoloģijām saskaņā ar jaunākajiem sasniegumiem;

b) kas ietver augsta līmeņa risku un apgrūtina datu subjektiem izmantot savas tiesības;

c) ja personas dati tiek apstrādāti, lai pieņemtu lēmumus attiecībā uz konkrētām fiziskām personām pēc jebkādas ar fiziskām personām saistītu personisku aspektu sistemātiskas un plašas novērtēšanas, kuras pamatā ir minēto datu profilēšana, vai pēc īpašu kategoriju personas datu apstrādes, biometrisko datu apstrādes vai tādu datu apstrādes, kas attiecas uz sodāmību un pārkāpumiem, vai ar tiem saistītiem drošības pasākumiem.

d) kas ietver augsta līmeņa risku, jo tās kavē attiecīgās personas īstenot savas tiesības vai izmantot pakalpojumu vai līgumu;

e) kas rada augstu risku, jo tās sistemātiski tiek veiktas plašā mērogā.

### NIDA veikšana vairāku līdzīgu apstrādes darbību kopumam

35.panta 1.punkts nosaka, ka vienota NIDA var tikt veikts apstrādes darbību kopumam ar līdzīgu riska pakāpi. Novērtējot šādu līdzību, jāņem vērā datu apstrādes vispārējais mērķis katrā atsevišķā gadījumā. 92.apsvērumā ir norādīts, ka, apsverot ekonomiskās izmaksas, NIDA var būt tematiski plašāks, dodot dalībniekiem kādā rūpniecības nozarē vai segmentā iespēju aptvert lietotņu vai apstrādes vidi vai plaši lietotas horizontālas darbības ar vienu NIDA.

### Pozitīvie un negatīvie saraksti NIDA veikšanai

Var pieņemt, ka uzraudzības iestādes publicēs pozitīvus vai negatīvus sarakstus, lai atvieglotu lēmuma pieņemšanu par NIDA nepieciešamību konkrētā gadījumā. Šie saraksti noteiks apstrādes veidus, kuriem nepieciešams NIDA ("pozitīvie saraksti") un gadījumi, kad nav nepieciešams NIDA ("negatīvie saraksti"). Kā daļa no regulatīvās saskaņotības, kas nodrošinātu labāku saskaņošanu visā ES, abi saraksti nacionālajām uzraudzības iestādēm jānosūta Eiropas Datu aizsardzības kolēģijai (35.panta 4.punkts),

Jāatzīmē, ka 29.panta darba grupa (DG29) iesaka veikt NIDA arī gadījumos, kad šķiet neskaidri, vai NIDA ir nepieciešams, lai izpildītu likumdošanas prasības pienācīgai datu aizsardzības nodrošināšanai.

## Kad jāveic NIDA?

Kad un ar kādām metodēm veikt NIDA, nosaka pārzinis. Par NIDA neizpildīšanu ir paredzētas juridiskas sankcijas, tāpēc ieteicams sākt sagatavošanos NIDA pēc iespējas ātrākā projekta posmā. Katram departamentam vai attiecīgajiem darbiniekiem, kas iesaistīti datu apstrādē, jāuzsāk attiecīgie procesi. Ieteicama apmācība, lai palielinātu izpratni par NIDA nepieciešamību organizācijā.

Apsverot riska samazināšanas pasākumus jebkura projekta, kas saistīts ar datu apstrādi, agrīnajā stadijā, var palīdzēt birokrātiskās darbības saglabāt samērā zemā līmenī.

NIDA var palīdzēt ceļā uz atbilstošu risinājumu atrašanu un var palīdzēt, kā minēts iepriekš, efektīvi un savlaicīgi īstenot datu aizsardzības prasības, izmantojot atbilstošus tehnoloģiskos risinājumus (integrētu datu aizsardzību) un noklusējuma iestatījumu izvēli, ņemot vērā datu aizsardzību.

Nodrošinot plašus un intensīvus sagatavošanās darbus, NIDA vadīs paredzēto projektu no agrīnās idejas posma līdz tā galīgās darbības ieviešanai un parādīs, ka NIDA procesam ir atkārtošanās raksturs.

Atvērts jautājums paliek, vai NIDA bija nepieciešams apstrādei, kas veikts pirms VDAR vispārējās piemērojamības (pirms 2018.gada 25.maija). Ņemot burtisko formulējumu ("pirms"), NIDA ir nepieciešams tikai tiem procesiem, kas tika uzsākti pēc 2018.gada 25.maija vai kas būtiski mainījušies pēc šī datuma.

Tā kā šajos gadījumos datu apstrādes sistēma jau darbojas, iepriekšēja pārbaude nav iespējama. Turklāt šīs darbības nepastāv neregulētā telpā (pieņemot, ka ir ņemti vērā visi iepriekšējā tiesiskā regulējuma noteikumi un pārskatu sniegšanas prasības).

Tomēr DG29 stingri iesaka veikt NIDA tām apstrādes darbībām, kas jau tiek veiktas, lai izvairītos no juridiskām neskaidrībām un pat juridiskām sankcijām.

## NIDA pārskatīšana

Pēc tam, kad NIDA ir veikts, ierosināto pasākumu īstenošana ir jāpārskata. Ja tiek uzskatīts par nepieciešamu, iespējams, būs jāveic pašas datu apstrādes pārskatīšana, lai identificētu jebkādus jaunus ar datu apstrādi saistītos risku elementus. 89.apsvērumā ir norādīts, ka NIDA pārskatīšana var būt neieciešama savlaicīgi pēc sākotnējā novērtējuma. Veicot NIDA, dokumentācijā vajadzētu iekļaut laika posmus, pēc kuriem veicama NIDA kārtējā pārbaude vai atjaunošana nākotnē.

Jāņem vērā tehnoloģiju attīstība, jauns tiesiskais regulējums un izmaiņas apstrādes kārtībā. Ja iestājas risks, ir jāveic jauns NIDA.

Pienākums veikt NIDA ir daļa no datu pārziņa pienākumiem, dokumentējot to pārskatatbildību. Dokumentācijā un pārskatā jānorāda ne tikai informācija par veikto NIDA, bet arī jāuzskaita jebkādi iemesli, kāpēc nav pabeigts pilns NIDA vai pārtraukts NIDA pēc tam, kad konstatēti lieli riski datu subjektiem.

## Apspriešanās ar datu uzraudzības iestādi saskaņā ar VDAR 36.pantu

Datu pārzinim ir jākonsultējas ar datu aizsardzības iestādi (DAI), ja NIDA atklāj augstus riskus un ja pārzinis nezina, kā veikt attiecīgus pasākumus, lai mazinātu šādus riskus. DAI ir jāreaģē uz šo pieprasījumu apspriesties četrpadsmit nedēļu laikā. Sarežģītiem un inovatīviem projektiem ir ieteicams pēc iespējas agrāk uzsākt NIDA, lai jebkuru DAI ieteikumu varētu ņemt vērā projekta plāna īstenošanā.

# Kas ir atbildīgs par NIDA veikšanu?

## Pamati

Par NIDA veikšanu atbildīgs ir pārzinis - šajā gadījumā vietējā pašvaldība. Sākotnēji Komisijas priekšlikums bija uzticēt NIDA datu apstrādātājam, kas rīkojas pārziņa uzdevumā. Savukārt 95.apsvērums tikai prasa, lai nepieciešamības gadījumā un pēc pieprasījuma apstrādātājs palīdzētu pārzinim nodrošināt, ka tiek ievēroti pienākumi, kas izriet no NIDA veikšanas.

Tāpēc praksē būtu lietderīgi līgumā paredzēt apstrādātāja iesaisti un aktīvu atbalstīšanu NIDA procesā. Tas būtu arī saskaņā ar 28.panta 3.punkta f) apakšpunktu, kas paredz, ka līgumā par apstrādi (vai citā juridiskā aktā) jāparedz, ka apstrādātājs palīdz pārzinim nodrošināt 32. līdz 36.pantā minēto pienākumu izpildi, ņemot vērā apstrādes veidu un apstrādātājam pieejamo informāciju;

Bieži vien tikai apstrādātājam būs nepieciešamā informācija, lai novērtētu attiecīgos apstrādes aspektus. Šajā gadījumā jāņem vērā tirdzniecības un uzņēmējdarbības noslēpumu atklāšanas risks, tāpēc ieteicams iekļaut atbilstošu līguma noteikumu, kas to atrunā. Ja paredzēta datu apstrāde, ko veic kopīgi pārziņi, NIDA saskaņā ar 35.panta 1.punkta 2.daļu, var veikt arī viens no pārziņiem - tas neatbrīvo citus pārziņus no pienākumiem.

## Piedalīšanās NIDA

NIDA ir jāorganizē kā projekts, un tādēļ tam vajadzētu būt aprīkotam ar nepieciešamajiem materiālajiem un cilvēkresursiem ar atbilstošu augsta līmeņa vadību. Veidojot projekta komandu, īpaša uzmanība jāpievērš projekta sarežģītībai, nepieciešamajām speciālista zināšanām un nepieciešamajām zināšanām par konkrēto projektu un tā vidi. Praksē var apvienot komandu, ko veido jurists, IT darbinieks, galvenais IT drošības speciālists, datu aizsardzības speciālists, departaments, kas pieprasījis apstrādi ("datu īpašnieks") utt.

Īpaša uzmanība tiek pievērsta tam, lai tiktu novērsti interešu konflikti. Tādējādi tie, kas nodarbojas ar datu apstrādi, nākotnē nav uzskatāmi par neatkarīgiem, bet, no otras puses, var sniegt vērtīgu ieguldījumu privātuma ietekmes novērtējuma izstrādē. Īstenošanu var veikt gan iekšējā komanda, gan pieaicinātas trešās personas. Ideālā gadījumā būtu jāiesaista neatkarīga institūcija.

Pārzinim ir jāvēršas pie datu aizsardzības speciālista pēc padoma. Saskaņā ar 39.panta 1.punkta c) apakšpunktu padomi par NIDA un tā īstenošanas uzraudzību ir datu

aizsardzības speciālista noteiktie pienākumi, bet tikai pēc pieprasījuma un nevis vadošā pozīcijā.

Tāpēc pārzinim ir pienākums saņemt padomu no datu aizsardzības speciālista. Kādā laikā un kādā mērā iesaistīt datu aizsardzības speciālistu, ir pārziņa lēmums. Vēlāk tam būtu jāpārskata arī gala ziņojums. Praksē ir ieteicams savlaicīgi iesaistīt datu aizsardzības speciālistu, jo viņa ekspertīze sākotnēji lieti noderēs.

Atkarībā no pārziņa organizācijas, ieteicams, lai NIDA apstiprinātu vadības līmenī vai attiecīga pilnvarota persona.

# Kā veikt NIDA?

## Pamati

Jāuzsver, ka VDAR nenosaka konkrētu veidu vai metodi, kādā izstrādāt NIDA, ko pašlaik intensīvi apspriež gan nacionālajos, gan Eiropas līmenī. DG29 norāda - lai izpildītu VDAR prasības var izmantot dažādas metodes un atsaucas uz esošo (vispārīgo vai nozaru) NIDA procesu sistēmu piemēriem, kas uzskaitīti pamatnostādņu par NIDA veikšanu 1.pielikumā[[2]](#footnote-2).

## NIDA īstenošana

Pārzinim principā ir brīva izvēle, kā īstenot NIDA procesu. Tādējādi to var pielāgot esošajām iekšējām procedūrām, ja pašvaldība ņem vērā četras prasības, kas ietvertas VDAR 35.panta 7.punktā no a) līdz d) apakšpunktam (sk. zemāk 4.3.punktu), kā NIDA obligātās prasības, kuras 29.panta darba grupa sīkāk skaidro, un papildus ņem vērā arī "iesaistītās puses" aspektu (sk. 35.panta 2.punktu) un datu subjektu viedokli (sk. 35.punkta 9.apakšpunkts).

## NIDA minimālais saturs

VDAR 35.panta 7.punkta a) līdz d) apakšpunkti kopā ar 84. un 90.apsvērumu kā minimumu nosaka:

a) plānotās apstrādes darbības un apstrādes nolūki, tostarp attiecīgā gadījumā pārziņa leģitīmo interešu sistemātisks apraksts;

b) novērtējums par apstrādes darbību nepieciešamību un samērīgumu attiecībā uz nolūkiem;

c) novērtējums par 1. punktā minētajiem riskiem datu subjektu tiesībām un brīvībām; un

d) pasākumi, kas paredzēti risku novēršanai, tostarp garantijas, drošības pasākumi un mehānismi, ar ko nodrošina personas datu aizsardzību un uzskatāmi parāda, ka ir ievērota šī regula, ņemot vērā datu subjektu un citu attiecīgo personu tiesības un leģitīmās intereses.

c) un d) apakšpunkti ir VDAR tā sauktās "uz risku balstītas pieejas" izpausmes, kas attiecas ne tikai uz NIDA īstenošanu, bet arī uz VDAR 24., 25. un 32.panta kontekstu. Citiem vārdiem sakot, NIDA ir īpašs piemērs uz risku balstītai pieeja tādu datu apstrādei, kas varētu izraisīt augstu risku fizisku personu tiesībām un brīvībām, un kurai nepieciešams veikt plašāku risku novērtējumu un rast risinājumus. Principā tomēr jebkurai citai datu apstrādes pieļaujamības pārbaudei arī nepieciešams riska novērtējums, ieskaitot atbilstīgus tehniskos un organizatoriskos pasākumus, kas samazina risku, pirms tā tiek īstenota (skatīt VDAR 24.panta 1.punktu).

## NIDA process

NIDA ir jāuztver kā process (ne tikai kā ziņojums), kas pēc iespējas drīzāk jāuzsāk, lai ietekmētu “projekta” izstrādi. Rezultātā novērtējums uz ietekmi gan atšķiras no audita, kas veic projekta pēckontroli, kad jau ir pārāk vēlu, lai risinātu datu aizsardzības vajadzības, kas būtu jādara NIDA.

Šobrīd ir daudz priekšlikumu NIDA procesa ieviešanai, kas vienā vai otrā veidā ir līdzīgi PIAF projekta ietvaros veiktā pētījuma rezultātiem (2012.g.)[[3]](#footnote-3), kurā tika apkopotas ietekmes uz privātuma novērtējumu (IPN) metodoloģijas septiņās valstīs (tostarp "labās prakses” ieteikumi un IPN procesa galvenie elementi) ES Komisijai. Tika noteikti šādi galvenie elementi:

1. IPN nepieciešamības noteikšana (sliekšņa analīze).
2. IPN komandas un darba uzdevuma noteikšana.
3. Ierosinātā projekta apraksts (un ieinteresēto personu noteikšana).
4. Informācijas plūsmu un citu ietekmes uz privātumu faktoru analīze.
5. Konsultācijas ar ieinteresētajām personām (“stakeholders”).
6. Riska vadība (risku identificēšana un iespējamie risinājumi).
7. Tiesiskās atbilstības pārbaude.
8. Ieteikumu formulēšana.
9. Ziņojuma sagatavošana un publicēšana (piemēram, organizācijas tīmekļa vietnē).
10. Ieteikumu īstenošana.
11. Ārējais (trešās personas) novērtējums un/vai audits.
12. IPN pārskatīšana, ja attiecīgais projekts mainās (IPN atjaunināšana, ja projektā ir izmaiņas).

NIDA modelis viedajiem tīkliem un viedās uzskaites sistēmām, kas norādīts Eiropas Komisijas Ieteikumā 2014/724/ES, paredz šādus darbības soļus:[[4]](#footnote-4)

1. solis Iepriekšējs novērtējums un kritēriji, kas nosaka nepieciešamību veikt NIDA
2. solis Uzsākšana
3. solis Viedo tīklu sistēmu vai lietojumprogrammu, ar ko apstrādā personas datus, identifikācija, raksturojums un apraksts.
4. solis Attiecīgo risku identificēšana.
5. solis Datu aizsardzības risku novērtējums.
6. solis Kontroles un atlikušo risku identificēšana un ieteikumi.
7. solis Dokumentēšana un NIDA ziņojuma izstrāde.
8. solis Pārskats un uzturēšana.

Jaunais ISO/IEC 29134 standarts sniedz vadlīnijas IPN veikšanai un ziņojuma struktūrai un saturam. Process ir sadalīts šādos četros apakšprocesos:

1. Sliekšņa analīze.
2. IPN sagatavošana.
3. IPN īstenošana.
4. IPN pārbaude.

Kādās un cik daļās NIDA process sadalāms, ir drīzāk gaumes jautājums. Citi ieteikumi piedāvā variācijas ar trim vai četriem posmiem, vēl citi - no sešiem līdz septiņiem

posmiem. Drīzāk svarīga ir procesa saprotamā struktūra un process, kurā jo īpaši tiek ņemts vērā VDAR 35.panta 7.punkts un 29. panta darba grupas ieteikumi.

## Datu subjektu vai to pārstāvju iekļaušana

Saskaņā ar 35.panta 9.punktu, attiecīgā gadījumā pārzinis pieprasa datu subjektu vai viņu pārstāvju viedokli par plānoto apstrādi, neskarot komerciālu vai sabiedrības interešu aizsardzību vai apstrādes darbību drošību. Vārdu "attiecīgā gadījumā" iekļaušana rada neskaidrības par to, pie kādiem nosacījumiem jāgūst attiecīgās personas vai tā pārstāvja viedoklis un kādos gadījumos (pieļaujams) to var nedarīt.

Veids, kādā šo viedokli pieprasīt, ir konteksta sensitīvs, un 29.darba grupa atpazīst dažādus tā veikšanas veidus, piemēram, veicot pētījumu (iekšējo vai ārējo), oficiālas intervijas ar personāla pārstāvjiem vai arodbiedrībām un nosūtot aptaujas pārziņa nākamajiem klientiem. No formulējuma izriet, ka viedokli iespējams tikai iegūt, bet nav pienākuma ņemt to vērā vai prasība par (jaunas) piekrišanas saņemšanu. Tomēr pārzinim būs jāņem vērā datu subjektu vai viņu pārstāvju viedokļi novērtējumā uz ietekmi. Literatūrā ir strīdīgs jautājums par to, vai patērētāju aizsardzības biedrības var tikt apzīmētas ar terminu "pārstāvis"[[5]](#footnote-5).

Jebkurā gadījumā pienākums konsultēties *expressis verbis* neskar komerciālu vai sabiedrības interešu aizsardzību vai apstrādes darbību drošību. Tāpēc pārzinis ārkārtas gadījumā var ierobežot vai atteikt pienākumu sniegt informāciju par paredzēto apstrādi attiecīgajām personām vai to pārstāvjiem saskaņā ar 35.panta 9.punktu (kas pēdējā gadījumā radīs situāciju, kad *a priori* iesaiste 35.panta 9.punkta izpratnē nebūs iespējama, jo pietiekamas informācijas esamība ir priekšnoteikums attiecīgo personu vai to pārstāvju viedokļa iegūšanai).

NIDA īstenošanai pierādījumu nolūkā ziņojumā ieteicams dokumentēt, kāpēc nav iegūts subjekta/tā pārstāvja viedoklis vai iegūts ierobežota satura viedoklis, vai iegūtais viedoklis nav ņemts vērā vai tikai daļēji ņemts vērā.

## Ziņojums par NIDA

Šajā brīdī jāatzīmē, ka NIDA ziņojums nav NIDA faktiskais mērķis, bet gan "līdzeklis mērķa sasniegšanai", lai dokumentētu procesu (iekšējo un ārējo). Ziņojumu nevajadzētu novērtēt par zemu - tas dokumentē īstenošanu un rezultātus, un, lai panāktu atbilstību, jāizvairās no "PR NIDA ziņojuma". Ziņojums var kalpot arī kā NIDA vadlīnijas un kontrolsaraksts.

Nedaudz pārsteidzoši, bet VDAR 35.pantā nav skaidras prasības sagatavot ziņojumu par NIDA veikšanu. Tomēr fakts, ka pārzinim ir dokumentācijas pienākums ir neapšaubāms un netieši izriet no VDAR 35.panta 7.punkta, kā arī no VDAR 5.panta 2.punkta (pārskatatbildība) kopā ar VDAR 24.panta 1.punktu un 36.panta 3.punkta e) apakšpunktu (kas paredz, ka pārzinis iesniedz uzraudzības iestādei " 35. pantā paredzēto novērtējumu par ietekmi uz datu aizsardzību"). Arī 35.panta 11.punktā pieprasītajam pārskatam, lai novērtētu, vai apstrāde tiek veikta saskaņā ar NIDA, nepieciešams, lai novērtējuma uz ietekmi rezultāti tiktu saglabāti. Turklāt ziņošana par IPN notiek saskaņā ar pasaules labo praksi šajā jomā (sk. sadaļu 4.1. augstāk), kas acīmredzami ir balstīta uz VDAR 35.punktā paredzēto NIDA.

Ieteicams NIDA procesā iekļaut "dzīvā dokumenta" (dokuments, kas tiek pastāvīgi rediģēts un atjaunināts) pieeju, sākot jau ar sliekšņa vērtības analīzes dokumentāciju, ja konstatēts, ka NIDA nav jāveic. Pat ja šī analīze parāda, ka NIDA nav nepieciešams un process tiek pārtraukts, pārzinis būs atbildīgs par atbilstību tam un pierādījumiem. Šo rakstisko dokumentāciju var iesniegt vadītājam jebkurā turpmākajā procesā un sekot līdzi iekšējiem apsvērumiem un novērtējumiem.

Attiecībā uz saturu NIDA ziņojumā būtībā ir noteikta procedūra (ieskaitot faktu izklāstu, sistemātiska apraksta veidā par visu testa priekšmetu - "novērtēšanas mērķis") un NIDA procesa rezultāti. Tāpat kā NIDA procesa gadījumā VDAR neparedz nekādus īpašus noteikumus NIDA ziņojuma sagatavošanā. Tomēr minimālā satura kritēriji ir noteikti DG29 pamatnostādņu WP 248 2.pielikumā, kas balstīti uz 35.panta 7.punktu. ISO/IEC 29134 iesaka sekojošu ziņojuma saturu ietekmes uz privātuma novērtējumam, koncentrējoties uz riska novērtējumu:

1. Atbilstošas privātuma prasības.
2. Darbības jomas apraksts.
3. Izmantoto riska kritēriju apraksts.
4. Īstenošanas dalībnieki.
5. Ieinteresētās puses, ar kurām notikušas konsultācijas.

To apstiprina arī 90.apsvērums, kurā cita starpā ir teikts: "Minētajā novērtējumā par ietekmi jo īpaši būtu jāietver paredzētie pasākumi, aizsardzības pasākumi un mehānismi, kas mazina minēto risku, nodrošina personas datu aizsardzību un uzskatāmi parāda, ka šīs regulas noteikumi ir ievēroti."

Ļoti detalizētajā PIAF pētījumā IPN ziņojuma minimālais saturs ir šāds:[[6]](#footnote-6)

1. Ievads un pamatinformācija, tostarp personas, kas apņēmušās veikt IPN, to kontaktinformācija un kur atrast papildu informāciju un citus palīdzības un padomu avotus.
2. Projekta, informācijas plūsmas un ietekmes uz privātumu apraksts.
3. Konsultāciju ar ieinteresētajām personām rezultāti.
4. Risku novērtējuma un risku samazināšanas posmu apraksts, ieskaitot iespējamās alternatīvas.
5. Tiesiskās atbilstības analīze.
6. Ieteikumi.
7. Pielikumi, ja nepieciešams.

Ja ir pieejams ziņojums vai projekta gala versija, var rasties jautājums par to, kas notiek ar atbildīgo personu (iekšēji), jo īpaši par to, vai kāds un kurš to "apstiprina" - praktiski svarīgs jautājums, kas paliek neminēts VDAR. Savā prakses kodeksā ICO (Informācijas lietu komisāra birojs Apvienotajā karalistē) ir skaidri noteicis: "iegūt atbilstošu apstiprinājumu organizācijā". Tā kā atbildīgajai personai ir jāveic NIDA, no tā izriet, ka NIDA ir iesaistīti attiecīgi atbildīgās personas pilnvaroti pārstāvji, un tiem ir arī galīgā atbildība. Vadības līmenim parasti būs galīgā lēmuma pieņemšanas pilnvaras par NIDA projekta priekšmetu un būtību. Minimālajā variantā projekta vadībai vai datu aizsardzības speciālistam jāziņo "augstākajam vadības līmenim", kā paredzēts VDAR 38.panta 3.punktā.

VDAR nav iekļauts pienākums publicēt NIDA, bet DG29 iesaka to publicēt (vismaz daļēji), lai palielinātu uzticību datu apstrādei un veicinātu pārredzamību. Jo īpaši publikācija ir ieteicama gadījumos, kad daļu no sabiedrības ietekmēs (plānotā) apstrāde.

# Secinājumi un praktiski padomi

Īpaši labi finansētas regulatīvās aģentūras gadu gaitā ir izstrādājušas savu pieeju novērtējumam par ietekmi uz datu aizsardzību (NIDA). No šodienas viedokļa var sagaidīt, ka tās datu aizsardzības iestādes, kuras jau ir izstrādājušas savu modeli, izvēlas vai popularizē to, jo attiecīgajai uzraudzības iestādei ir visizteiktākās zināšanas par saviem ieteikumiem. Šobrīd pieejamo nacionālo uzraudzības iestāžu (no ES dalībvalstīm) modeļu saturs lielā daļā gadījumu tika sagatavots pirms VDAR, un tie (vēl) nav konsekventi pielāgoti VDAR prasībām vai terminoloģijai.

Tomēr ICO (Informācijas lietu komisāra birojs Apvienotajā karalistē) pievienoja savu ietekmes uz privātuma novērtējuma prakses kodeksu (2014.g.) ziņojumam (kuru vērts izlasīt) "Lielie dati, mākslīgais intelekts, datormācīšanās un datu aizsardzība" atbilstoši VDAR prasībām un terminoloģijai, kas tiek sagaidīts arī no citām datu aizsardzības iestādēm. Atklāts paliek jautājums, vai Eiropas Datu aizsardzības kolēģija (68.pants) sagatavos NIDA pamatnostādnes, ieteikumus un/vai paraugpraksi saskaņā ar 70.panta 1.punkta e) apakšpunktu.

Ieteikumi īsumā:

* Visu lēmumu dokumentēšana, jo īpaši, kāpēc NIDA nav veikts (ja piemērojams);
* Ja rodas šaubas, veiciet NIDA;
* Iekšējo un ārējo ieinteresēto personu iesaistīšana;
* Izmantojiet paraugus, labo praksi un, ja nepieciešams, līdzīgu NIDA, kas jau izveidots;
* NIDA publicēšana:
  + Īpaši ieteicams publiskām iestādēm;
  + Palielina informētību par privātumu un palielina uzticēšanos.

# Ārējie avoti un tīmekļa vietnes

## Grāmatas un publikācijas

* ***Kastelitz, M., Hötzendorfer, W., Riedl, R***., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, 113ff.
* ***De Hert, Paul/Kloza, Dariusz/Wright, David,*** Recommendations for a privacy impact assessment framework for the European Union   
  <http://www.piafproject.eu/ref/PIAF_D3_final.pdf>
* ***Wright, David*/*De Hert, Paul* (Ed.),** Privacy Impact Assessment, Springer Science & Business Media, Dordrecht, Heidelberg, London, New York 2012
* ***De Hert/Kloza/Wright*** (Ed.), **PIAF**, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012), http://piafproject.eu/ref/PIAF\_D3\_final.pdf; vairāk informācijas pieejams <http://piafproject.eu/Deliverables.html>.
* ***Martini in Paal/Pauly*** (Ed.), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

## 29.panta darba grupas dokumenti

* 29.darba grupa, WP 248, 2017.gada 4.aprīlī: Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA) veikšanai un noskaidrošanai, vai apstrāde “varētu radīt augstu risku” Regulas 2016/679 izpratnē <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236>

## Tīmekļa saites

* Brussels Laboratory for Data Protection and Privacy Impact Assessments  
  <http://www.vub.ac.be/LSTS/dpialab/>
* ICO, Big data, artificial intelligence, machine learning and data protection (2017), 99 f, <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.

1. Turpmākais teksts balstīts uz publikāciju vācu valodā: Kastelitz, M., Hötzendorfer, W., Riedl, R., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, 113ff. [↑](#footnote-ref-1)
2. DG29, WP 248: Var izmantot dažādas metodikas (skatīt pamatnostādņu 1.pielikumu NIDA metodoloģiju piemēriem), lai palīdzētu īstenot VDAR izklāstītās pamatprasības. [↑](#footnote-ref-2)
3. *De Hert/Kloza/Wright* (Hrsg), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012), http://piafproject.eu/ref/PIAF\_D3\_final.pdf; vairāk informācijas <http://piafproject.eu/Deliverables.html>. [↑](#footnote-ref-3)
4. Komisijas ieteikums 2014/724/ES par datu aizsardzības ietekmējuma novērtējuma veidlapu viedajiem tīkliem un viedās uzskaites sistēmām, 2014.gada 10.oktobris, L 2014/300, 63. [↑](#footnote-ref-4)
5. *Martini* in Paal/Pauly (Hrsg), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99. [↑](#footnote-ref-5)
6. *De Hert/Kloza/Wright* (Hrsg), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012) 31, http://piafproject.eu/ref/PIAF\_D3\_final.pdf. [↑](#footnote-ref-6)