*Datu aizsardzības speciālista (DAS) iecelšana, amats un funkcijas*

Saturs

[1. TIESISKAIS REGULĒJUMS 4](#_Toc516251366)

[VDAR 4](#_Toc516251367)

[2. DAS IECELŠANA 7](#_Toc516251368)

[2.1. Obligāta iecelšana saskaņā ar VDAR 7](#_Toc516251369)

[2.1.1. Publiska iestāde vai struktūra 7](#_Toc516251370)

[2.1.2. Pārziņa vai apstrādātāja pamatdarbība […], kurai nepieciešama regulāra un sistemātiska datu subjektu novērošana plašā mērogā 7](#_Toc516251371)

[2.1.3. Pārziņa vai apstrādātāja pamatdarbības ietver īpašo kategoriju datu […] un personas datu par sodāmību un pārkāpumiem apstrādi plašā mērogā 8](#_Toc516251373)

[2.2. DAS iecelšana citās situācijās 9](#_Toc516251374)

[2.2.1. Obligātā iecelšana saskaņā ar ES vai dalībvalstu tiesību aktiem 9](#_Toc516251375)

[2.2.2. Brīvprātīga iecelšana 9](#_Toc516251376)

[2.3. Līgumiskās attiecības ar DAS 10](#_Toc516251377)

[2.3.1. Darba līgums 10](#_Toc516251378)

[2.3.2. Pakalpojuma līgums 10](#_Toc516251379)

[3. DAS AMATS 10](#_Toc516251380)

[3.1. Iesaistīšana visos jautājumos, kas saistīti ar personas datu aizsardzību 10](#_Toc516251381)

[3.2. Nepieciešamo resursu un neatkarības nodrošināšana 11](#_Toc516251382)

[3.3. Interešu konflikts 12](#_Toc516251383)

[4. DAS UZDEVUMI 13](#_Toc516251384)

[4.1. Uzraudzība 13](#_Toc516251385)

[4.2. Novērtējums par ietekmi uz datu aizsardzību (NIDA) 13](#_Toc516251386)

[4.3. Kontaktpunkts 13](#_Toc516251387)

[4.4. Datu uzglabāšana 14](#_Toc516251388)

[5. SECINĀJUMI UN PRAKTISKIE PADOMI 14](#_Toc516251389)

[6. ĀRĒJIE AVOTI UN TĪMEKĻA VIETNES 15](#_Toc516251390)

[Grāmatas 15](#_Toc516251391)

[29.panta darba grupas dokumenti 15](#_Toc516251392)

[Tīmekļa saites 15](#_Toc516251393)

[7. ATSAUCES 15](#_Toc516251394)

# TIESISKAIS REGULĒJUMS

## VDAR

*97.apsvērums*

*Ja datu apstrādi veic publiska iestāde, izņemot tiesas vai neatkarīgas tiesu iestādes, kad tās pilda tiesas funkciju, ja privātajā sektorā apstrādi veic pārzinis, kura pamatdarbības sastāv no apstrādes darbībām, kam nepieciešama regulāra un sistemātiska datu subjektu novērošana plašā mērogā, vai ja datu pārziņa vai apstrādātāja pamatdarbības ietver īpašo kategoriju personas datu un datu par sodāmību un pārkāpumiem apstrādi plašā mērogā, personai ar speciālām zināšanām datu aizsardzības tiesību un prakses jomā būtu jāpalīdz pārzinim vai apstrādātājam uzraudzīt to, kā iekšēji tiek ievērota šī regula. Privātajā sektorā pārziņa pamatdarbības ir saistītas ar tā galvenajām darbībām, un tās nav saistītas ar personas datu apstrādi kā palīgdarbības. Nepieciešamais speciālo zināšanu līmenis būtu jānosaka jo īpaši saskaņā ar veiktajām datu apstrādes darbībām un aizsardzību, kas nepieciešama personas datiem, kurus pārzinis vai apstrādātājs apstrādā. Šādiem datu aizsardzības speciālistiem neatkarīgi no tā, vai pārzinis ir to darba devējs, būtu jāspēj neatkarīgi pildīt savus pienākumus un uzdevumus.*

*37.pants*

*Datu aizsardzības speciālista iecelšana*

*1. Pārzinis un apstrādātājs ieceļ datu aizsardzības speciālistu katrā gadījumā, kad:*

*(a) apstrādi veic publiska iestāde vai struktūra, izņemot tiesas, tām pildot savus uzdevumus;*

*(b) pārziņa vai apstrādātāja pamatdarbība sastāv no apstrādes darbībām, kurām to būtības, apmēra un/vai nolūku dēļ nepieciešama regulāra un sistemātiska datu subjektu novērošana plašā mērogā; vai*

*(c) pārziņa vai apstrādātāja pamatdarbības ietver īpašo kategoriju datu saskaņā ar 9. pantu un 10. pantā minēto personas datu par sodāmību un pārkāpumiem apstrādi plašā mērogā.*

*2. Uzņēmumu grupa var iecelt vienu datu aizsardzības speciālistu ar noteikumu, ka katrs uzņēmums var viegli sazināties ar datu aizsardzības speciālistu.*

*3. Ja pārzinis vai apstrādātājs ir publiska iestāde vai struktūra, vienu datu aizsardzības speciālistu var iecelt vairākām šādām iestādēm vai struktūrām, ņemot vērā to organizatorisko uzbūvi un lielumu.*

*4. Gadījumos, kas nav minēti 1. punktā, pārzinis vai apstrādātājs, vai apvienības un citas struktūras, kas pārstāv pārziņu vai apstrādātāju kategorijas, var iecelt vai – ja tas jādara saskaņā ar Savienības vai dalībvalsts tiesību aktiem – ieceļ datu aizsardzības speciālistu. Datu aizsardzības speciālists var rīkoties šādu apvienību un citu struktūru, kas pārstāv pārziņus vai apstrādātājus, uzdevumā.*

*5. Datu aizsardzības speciālistu ieceļ, pamatojoties uz viņa profesionālo kvalifikāciju, jo īpaši speciālām zināšanām datu aizsardzības tiesību un prakses jomā un spēju pildīt 39. pantā minētos uzdevumus.*

*6. Datu aizsardzības speciālists var būt pārziņa vai apstrādātāja darbinieks, vai viņš var veikt uzdevumus, pamatojoties uz pakalpojumu līgumu.*

*7. Pārzinis vai apstrādātājs publisko datu aizsardzības speciālista kontaktinformāciju un paziņo to uzraudzības iestādei.*

*38.pants*

*Datu aizsardzības speciālista statuss*

*1. Pārzinis un apstrādātājs nodrošina, ka datu aizsardzības speciālists tiek pienācīgi un laikus iesaistīts visos jautājumos saistībā ar personas datu aizsardzību.*

*2.   Pārzinis un apstrādātājs atbalsta datu aizsardzības speciālistu 39. pantā minēto uzdevumu izpildē, nodrošinot resursus, kas nepieciešami, lai veiktu minētos uzdevumus, un nodrošinot piekļuvi personas datiem un apstrādes darbībām, un lai viņš uzturētu speciālās zināšanas.*

*3.   Pārzinis un apstrādātājs nodrošina, ka datu aizsardzības speciālists nesaņem nekādus norādījumus attiecībā uz minēto uzdevumu veikšanu. Pārzinis vai apstrādātājs viņu neatlaiž vai viņam nepiemēro sankcijas par viņa uzdevumu veikšanu. Datu aizsardzības speciālists ir tieši atbildīgs pārziņa vai apstrādātāja augstākās vadības priekšā.*

*4.   Datu subjekti var vērsties pie datu aizsardzības speciālista visos jautājumos, kas saistīti ar viņu personas datu apstrādi un šajā regulā paredzēto tiesību īstenošanu.*

*5.   Datu aizsardzības speciālistam ir saistoša slepenības vai konfidencialitātes ievērošana saistībā ar viņa uzdevumu pildīšanu, kā paredzēts Savienības vai dalībvalstu tiesību aktos.*

*6.   Datu aizsardzības speciālists var pildīt citus uzdevumus un pienākumus. Pārzinis vai apstrādātājs nodrošina, lai neviens no minētajiem uzdevumiem un pienākumiem neradītu interešu konfliktu.*

*39.pants*

*Datu aizsardzības speciālista uzdevumi*

*1. Datu aizsardzības speciālistam ir vismaz šādi uzdevumi:*

*(a) informēt un konsultēt pārzini vai apstrādātāju un darbiniekus, kuri veic apstrādi, par viņu pienākumiem saskaņā ar šo regulu un ar citiem Savienības vai dalībvalstu noteikumiem par datu aizsardzību;*

*(b) uzraudzīt, vai tiek ievērota šī regula, citi Savienības vai dalībvalstu noteikumi par datu aizsardzību un pārziņa vai apstrādātāja politika saistībā ar personas datu aizsardzību, tostarp pienākumu sadali, apstrādes darbībās iesaistīto darbinieku informēšanu un apmācību, un ar to saistītajām revīzijām;*

*(c) pēc pieprasījuma sniegt padomus attiecībā uz novērtējumu par ietekmi uz datu aizsardzību un pārraudzīt tā īstenošanu saskaņā ar 35. pantu;*

*(d) sadarboties ar uzraudzības iestādi;*

*(e) būt par uzraudzības iestādes kontaktpunktu jautājumos, kas saistīti ar apstrādi, tostarp 36. pantā minēto iepriekšējo apspriešanos, un attiecīgā gadījumā konsultēt par jebkuru citu jautājumu.*

*2. Datu aizsardzības speciālists, pildot savus uzdevumus, pienācīgi ņem vērā ar apstrādes darbībām saistīto risku, ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūku.*

# DAS IECELŠANA

## Obligāta iecelšana saskaņā ar VDAR

### Publiska iestāde vai struktūra

VDAR nesatur juridisku definējumu, kas ir "publiska iestāde vai struktūra". Tam, vai konkrēta fiziska vai juridiska persona ir publiska iestāde vai struktūra, būtu jābūt noteiktam saskaņā ar attiecīgās dalībvalsts tiesību aktiem. Šis jēdziens jāinterpretē **plaši** un jebkurā gadījumā ietver valsts, reģionālās un **vietējās varas iestādes**. Tomēr saskaņā ar DG29 tas var ietvert arī noteiktas fiziskas vai juridiskas personas, kuru darbību regulē valsts vai privātās tiesības (piemēram, sabiedriskā transporta pakalpojumi, ūdensapgāde un energoapgāde, ceļu infrastruktūra, sabiedriskā apraide, valsts mājokļi vai reglamentētu profesiju disciplinārās iestādes)[[1]](#endnote-1). Šādas interpretācijas loģika ir tāda, ka pilsoņiem (datu subjektiem) ir ierobežota izvēle, vai un kā šādas iestādes apstrādās viņu personas datus. Lai gan šāda interpretācija nav obligāta un saistoša, šīm iestādēm ieteicams rūpīgi izskatīt un izanalizēt, vai tām iecelt DAS.

Jāatzīmē, ka DG29 kā labu praksi iesaka iecelt DAS, kura funkcijām vajadzētu attiekties arī uz visām veiktajām apstrādes darbībām, tostarp tām, kas nav saistītas ar publiskā uzdevuma veikšanu vai oficiālu pienākumu izpildi (piemēram, attiecības ar darbiniekiem)[[2]](#endnote-2). Tomēr nevienā no VDAR noteikumiem nav minēta prasība iecelt DAS tikai tām apstrādes darbībām, kas saistītas ar publiskām funkcijām. Tādējādi saprātīgākā un drošākā interpretācija ir tāda, kurā pašvaldības ieceļ DAS, **kurš ir atbildīgs par visām organizācijas datu apstrādes darbībām** (attiecības ar iedzīvotājiem, darbiniekiem, kandidātiem uz darba vietām, bijušajiem darbiniekiem, citām publiskām iestādēm utt.).

### Pārziņa vai apstrādātāja pamatdarbība […], kurai nepieciešama regulāra un sistemātiska datu subjektu novērošana plašā mērogā

Pašvaldību veiktā datu apstrāde galvenokārt notiek augstākminētā 2.1.1. punkta ietvaros, t.i., pašvaldībām būtu jāieceļ DAS, balstoties uz to publiskās iestādes vai struktūras kapacitāti. Skaidrības labad turpmāk tiks veikta īsa analīze par divām citām hipotēzēm saskaņā ar VDAR, kad DAS iecelšana ir obligāta. Šī informācija varētu būt noderīga privātām struktūrām, kuru kapitāls daļēji vai pilnīgi pieder pašvaldībai vai citām pašvaldību vai valsts struktūrām un kuras neietilpst "publiska iestāde vai struktūra" darbības laukā.

Ar terminu **"pamatdarbība"** var uzskatīt galvenās darbības, kas nepieciešamas, lai sasniegtu pārziņa vai apstrādātāja mērķus[[3]](#endnote-3). DG29 sniegtie piemēri ietver veselības datu apstrādi slimnīcās vai privātās apsardzes uzņēmuma veikto uzraudzību. No otras puses, darbinieku standarta IT atbalsta pasākumi tiek izslēgti no organizācijas "pamatdarbībām"[[4]](#endnote-4).

Jēdziens **"plašs mērogs"** nav skaidri definēts VDAR. Tajā ir skaidri norādīts, ka datu apstrāde reģionālā, valsts vai starpvalstu līmenī, kas ietver ievērojamu datu apjomu un kas var ietekmēt lielu datu subjektu skaitu un izraisīt augstu risku, var uzskatīt par "plaša mēroga" apstrādi. No otras puses, tādi speciālisti kā veselības aprūpes speciālists vai advokāts neapstrādā personas datus "plašā mērogā".

Saskaņā ar DG29, par plaša mēroga apstrādi var uzskatīt sekojošus piemērus:

* pacienta datu apstrāde slimnīcā;
* personu, kuras izmanto pilsētas sabiedrisko transportu, pārvietošanās datu apstrāde (piemēram, izsekošana ar braukšanas kartēm);
* starptautiskas ātrās ēdināšanas ķēžu klientu faktiskās ģeogrāfiskās atrašanās vietas datu apstrāde statistikas vajadzībām, ko veic šo pakalpojumu sniegšanas speciālists;
* klientu datu apstrāde, ko veic apdrošināšanas sabiedrība vai banka;
* personas datu apstrāde meklētājprogrammas paradumorientētai reklāmai
* datu apstrāde (saturs, transports, atrašanās vieta) pa tālruni vai caur interneta pakalpojumu sniedzējiem[[5]](#endnote-5).

Jēdziens **"regulārs"** būtībā ir saistīts ar apstrādi, kas notiek vai nu pastāvīgi vai periodiski. Jēdziens **"sistemātiska novērošana"** paģērē, lai apstrāde notiktu pēc konkrēta plāna, stratēģijas vai līdzīgas iepriekš noteiktas metodoloģijas organizētā veidā saskaņā ar sistēmu[[6]](#endnote-6). Kā piemēri ir telekomunikāciju tīklu operatori, profilēšana, paradumorientēta reklāma, viedās ierīces utt.



### Pārziņa vai apstrādātāja pamatdarbības ietver īpašo kategoriju datu […] un personas datu par sodāmību un pārkāpumiem apstrādi plašā mērogā

Jēdzienu “pamatdarbība” un “plašs mērogs” skaidrojumus skatiet augstāk punktā 2.1.2.

Vārds “un” interpretējams korektīvi kā "vai". Citiem vārdiem sakot, DAS iecelšana būtu nepieciešama organizācijā, kurā notiek īpašu kategoriju datu apstrāde **vai** personas datu par sodāmību un pārkāpumiem apstrāde plašā mērogā un kas ir organizācijas pamatdarbības daļa.

Īpašu kategoriju personas dati ir:

* personas dati, kuri atklāj rases vai etnisko piederību;
* politiskie uzskati;
* reliģiskā vai filozofiskā pārliecība;
* dalība arodbiedrībā;
* ģenētiskie dati;
* biometriskie dati, lai veiktu fiziskas personas viennozīmīgu identifikāciju;
* dati, kas attiecas uz veselību vai fiziskas personas dzimumdzīvi vai seksuālo orientāciju.

Personas dati par sodāmību un pārkāpumiem var ietvert informāciju, kas iekļauta tiesas spriedumos, sodāmības reģistrā, izmeklēšanas dienestu aktos.

## DAS iecelšana citās situācijās

### Obligātā iecelšana saskaņā ar ES vai dalībvalstu tiesību aktiem

Saskaņā ar VDAR 37.panta 4.punktu ES un/vai dalībvalstīm ir tiesības paredzēt citas situācijas, kad DAS iecelšana ir obligāta. Šāda obligāta iecelšana var būt nepieciešama pēc kvalitatīvām pazīmēm (piemēram, noteiktām nozarēm raksturīgām apstrādes darbībām) vai kvantitatīvām pazīmēm (piemēram, ja organizācija apstrādā personas datus noteiktam skaitam datu subjektu). Piemēram, Vācija savos datu aizsardzības tiesību aktos ir noteikusi plašākas prasības nekā VDAR: a) uzņēmumiem, kas veic uzņēmējdarbību Vācijā un iesaista vismaz 10 personas automatizētas apstrādes jomā, ir obligāti jāieceļ DAS; b) automatizētas apstrādes gadījumos, kas tiek veiktas uzņēmējdarbības gaitā datu pārsūtīšanas nolūkā, anonimizētai pārsūtīšanai, tirgum vai viedoklim, uzņēmumiem ir jāieceļ DAS neatkarīgi no personu skaita, kas tiek nodarbināti personas datu automatizētai apstrādei[[7]](#endnote-7).

### Brīvprātīga iecelšana

VDAR paredz arī iespēju brīvprātīgi iecelt DAS. Šādu pieeju varētu izmantot organizācijas, kuras vēlas parādīt savu atbilstību datu aizsardzības noteikumiem un veicināt pārredzamību un uzticēšanos. Tā kā pašvaldību darbība ietilpst pirmajā obligātajā prasībā (publiska iestāde vai struktūra), brīvprātīgu DAS iecelšanu var piemērot noteiktām organizācijām, kuru kapitāls pieder pašvaldībai vai valstij, piemēram, sabiedriskā transporta uzņēmumi, valsts skolas vai universitātes, sabiedrisko pakalpojumu sniedzēji (ūdens, gāze, elektroapgāde) u.c.

## Līgumiskās attiecības ar DAS

### Darba līgums

VDAR skaidri paredz iespēju iecelt DAS uz darba līguma pamata. Tas nozīmē divas iespējas: a) iecelt kādu personu, kas jau strādā organizācijā, apvienojot savas funkcijas ar DAS funkcijām vai b) izveidot DAS jaunu darba vietu. Izvēle starp šīm divām iespējām lielā mērā ir atkarīga no organizācijas struktūras, darbinieku skaita, darba slodzes un datu apstrādes veida un skaita, un būtu jāveic katram gadījumam atsevišķi. Ja kādas pašvaldības iestāde ir salīdzinoši maza (piemēram, atrodas mazā ciemā ar nelielu skaitu iedzīvotāju, kuru dati tiek apstrādāti), varētu būt pamatoti nepieņemt jaunu darbinieku, bet drīzāk piešķirt DAS funkcijas kādam, kas jau strādā organizācijā (jebkurā gadījumā jāizvairās no interešu konflikta). Gluži pretēji, ja pašvaldības iestāde ir liela un/vai tās ikdienas darbības saistītas ar ievērojamu personas datu apjomu (vai konfidenciālu datu vai datu saistībā ar sodāmību un pārkāpumiem) apstrādi, izvēle izveidot jaunu darba vietu (vismaz) vienam DAS šķiet pamatota.

### Pakalpojuma līgums

VDAR neuzliek par pienākumu organizācijām iecelt DAS tikai kā personāla locekļus. Regulā ir skaidri noteikts, ka DAS funkciju var veikt arī ārpakalpojuma sniedzējs (persona vai organizācija), ar kuru noslēgts pakalpojuma līgums. DG29 iesaka par labu praksi ārējai DAS komandai noteikt katram klientam vienu vadošo kontaktpersonu un "atbildīgo personu", kas būtu jānorāda pakalpojuma līgumā[[8]](#endnote-8). Turklāt ikvienam ārējās DAS organizācijas loceklim jāatbilst visām VDAR piemērojamajām prasībām.

Ārpakalpojuma sniedzēja piesaistīšana DAS funkciju veikšanai varētu būt saprātīga arī tāpēc, ka šādai organizācijai ir nepieciešamās ekspertu zināšanas, pieredze un visi atbilstošie sertifikāti[[9]](#endnote-9).

Visbeidzot, bet ne mazāk svarīgi, atkarībā no vietējās likumdošanas (piemēram, saskaņā ar publisko iepirkumu likumiem) pakalpojuma līguma noslēgšanai ar ārēju DAS varētu būt nepieciešama dažu formālu procedūru veikšana.

# DAS AMATS

## Iesaistīšana visos jautājumos, kas saistīti ar personas datu aizsardzību

VDAR skaidri nosaka, ka DAS jāiesaista visos jautājumos, kas saistīti ar personas datu aizsardzību organizācijā. DG29 saredz DAS iesaisti (konsultāciju, padomu, kontroles u.c. veidā) pēc iespējas ātrāk katrā procesā, kas ietver personas datu apstrādi, kā vienu no līdzekļiem, lai nodrošinātu konfidencialitāti saskaņā ar integrēto datu aizsardzības pieeju[[10]](#endnote-10).

Praktiski DAS iesaistīšana organizācijā varētu iekļaut piemēram:

* Padoma lūgšana, veicot novērtējumu par ietekmi uz datu aizsardzību (NIDA) (VDAR 35.panta 2.punkts);
* Dalība darba sanāksmēs (DG29 nosaka piedalīšanos augstākā un vidējā līmeņa vadības sanāksmēs, taču praksē DAS mijiedarbībai ar personālu ekspertu līmenī varētu būt līdzīga (ja ne augstāka) pievienotā vērtība);
* Konsultēšanās ar DAS ikreiz, kad tiek pieņemts vadības lēmums saistībā ar datu apstrādi;
* Konsultēšanās ar DAS par to, kādi pasākumi jāveic, ja rodas datu aizsardzības pārkāpums.

## Nepieciešamo resursu un neatkarības nodrošināšana

DAS nespētu pilnvērtīgi pildīt savus pienākumus, ja tas nebūtu nodrošināts ar nepieciešamajiem resursiem. Tāpēc organizācijas vadība ir atbildīga par to, lai DAS būtu pienācīgi nodrošināti šādi aspekti:

* **Orgnizatoriskie aspekti:**
  + DAS, veicot savas pienākumus, nepieciešama komanda, kas to atbalsta. Tas ir īpaši svarīgi lielākām organizācijām. Dažkārt vairāku DAS iecelšana varētu būt risinājums;
  + Piekļuve visām citām komandām organizācijā. DAS nespētu pienācīgi pildīt savus pienākumus, ja tas nevarētu pilnvērtīgi sadarboties ar visām citām ar datu apstrādi atbildīgajām grupām (piemēram, reģistru nodaļa un lietvedības departaments, juridiskais departaments, personāla daļa, grāmatvedība, IT departaments u.c.);
  + Atbildīgs tikai augstākās vadības priekšā. VDAR skaidri nosaka, ka DAS uzņemas atbildību tikai pret augstāko organizācijas vadību. Pašvaldību gadījumā tas varētu būt, piemēram, domes priekšsēdētājs, novada dome, attiecīgās administratīvās vienības direktors vai priekšsēdētājs utt. Šī prasība ir ļoti svarīga, lai nodrošinātu DAS neatkarību. Ja DAS saikne ar vadību būtu netieša (piemēram, izmantojot tādus starpniekus kā juridisko vai personāla daļas vadītāju), DAS nevarētu pienācīgi pildīt savus pienākumus, jo rastos situācija, kurā DAS ir atbildīgs pret kāda, kuru tam vajadzētu kontrolēt;
  + Pietiekams laiks, lai veiktu savus pienākumus. Tas ir īpaši svarīgi, ja DAS tiek iecelts uz nepilnu darba laiku, vai, ja darbinieks papildus citiem pienākumiem veic datu aizsardzību[[11]](#endnote-11). Kā labo praksi DG29 iesaka noteikt procentuālu laika daļu DAS pienākumiem, ja tā nav pilna slodze.
* **Finanšu aspekti**
  + DAS jābūt pieejamiem nepieciešamajiem finanšu resursiem, lai veiktu savas funkcijas. Ja organizācija nenodrošina pietiekamu budžetu datu aizsardzības pasākumiem, tas varētu apdraudēt DAS funkciju pienācīgu izpildi;
  + DAS jābūt pieejamai nepieciešamajai infrastruktūrai (telpām, datoriem, interneta pieslēgumam, datu bāzēm, tehniskajiem risinājumiem, piemēram, programmatūrām u.c.).
* **Izglītības aspekti** – DAS ekspertu zināšanu līmenis būtu pastāvīgi jāpaaugstina (izmantojot kursus, nodrošinot jaunu literatūru utt.). Ņemot vērā to, ka datu aizsardzība ir ļoti dinamiska zināšanu joma, ir saprotams, ka DAS jābūt informētam par jaunākajām tendencēm un attīstību, lai pienācīgi nodrošinātu pēc iespējas augstāku datu aizsardzības līmeni organizācijā un risinātu aktuālās problēmas tehnoloģiskās un juridiskās attīstības kontekstā.

Būtisks DAS neatkarības aspekts ir **aizliegums sodīt vai radīt jebkādas nelabvēlīgas sekas** DAS par savu pienākumu pildīšanu. Nelabvēlīgas sekas var atšķirties dažādās situācijās - no atlaišanas no darba vai cita veida disciplinārsoda līdz atteikumam par paaugstināšanu amatā, atteikums par pabalstiem, ko saņēmuši citi darbinieki utt. Var sagaidīt, ka dalībvalstis savā darba likumdošanā ieviesīs grozījumus un nodrošinās DAS aizsardzību pret atlaišanu laikā, kad tie pilda savas funkcijas, un kādu laika posmu pēc tam[[12]](#endnote-12). Tajā pašā laikā būtu jāpiemēro saprātīga šā aizlieguma interpolācija - DAS nevar sodīt par pienācīgu savu pakalpojumu sniegšanu. Tomēr, ja DAS trūkst nepieciešamo zināšanu un prasmju, tie veic disciplinārus pārkāpumus utt., organizācijām jābūt tiesīgām tos atlaist, pamatojoties uz jebkuru atlaišanas iemeslu, kas minēts attiecīgajā nacionālajā darba likumdošanā.

## Interešu konflikts

Ja DAS ir norīkots saskaņā ar darba līgumu, šim norīkojumam nevajadzētu radīt interešu konfliktu. Interešu konflikts varētu rasties, ja DAS pilda citus pienākumus organizācijā, kas nosaka datu apstrādes mērķus un līdzekļus iekšējā procesā. Citiem vārdiem sakot, DAS nevar būt vienlaikus direktors, izpilddirektors, finanšu vadītājs, galvenais ārsts, mārketinga nodaļas vadītājs, personāldaļas vadītājs vai IT nodaļas vadītājs[[13]](#endnote-13). Turklāt citi zemāki amati organizatoriskajā struktūrā arī var izraisīt interešu konfliktu, ja šādu pozīciju vai amatu ietvaros var tikt noteikti datu apstrādes mērķi un līdzekļi (piemēram, grāmatvedis, juridiskais konsultants, IT speciālists).

Interešu konflikts var rasties ne tikai, ja tiek noteikts DAS saskaņā ar darba līgumu, bet arī ārēja DAS gadījumā. Ja DAS tiek lūgts pārstāvēt datu pārzini vai apstrādātāju tiesā lietā, kas saistīta ar datu aizsardzības jautājumiem, var rasties interešu konflikts, jo pārzinim un apstrādātājam ir pretrunīgas intereses.

# DAS UZDEVUMI

## Uzraudzība

Viens no galvenajiem DAS uzdevumiem ir uzraudzīt visas datu apstrādes darbības organizācijā. Tas būtībā ir saistīts ar informācijas saņemšanu/apkopošanu, šīs informācijas iekšēju analīzi, kā arī paskaidrojumu, ieteikumu un padomu sniegšanu organizācijā. Uzraudzības funkcija ir vērsta uz iekšējiem procesiem organizācijā, tādēļ būtu jāinformē un jāsniedz padomi ne tikai vadībai, bet arī pastāvīgajiem darbiniekiem ekspertu līmenī, kuru pienākumi ir saistīti ar personas datu apstrādi.

## Novērtējums par ietekmi uz datu aizsardzību (NIDA)

VDAR nosaka, ka DAS tiek iesaistīts ar savām padomdevēja funkcijām NIDA. DG29 iesaka kā paraugpraksi lūgt DAS padomu par vienu vai vairākiem sekojošiem ar ietekmes novērtējumu saistītajiem jautājumiem:

* vai NIDA vispār ir jāveic;
* kāda metodika jāievēro, veicot NIDA;
* vai veikt iekšējo NIDA vai izmantot ārpakalpojumus;
* kādus drošības pasākumus (ieskaitot tehniskos un organizatoriskos pasākumus) piemērot, lai mazinātu datu subjektu tiesību un interešu riskus;
* vai NIDA ir ticis pareizi veikts un vai tā secinājumi ir saskaņā ar VDAR[[14]](#endnote-14).

Ja organizācijas vadība nolemj neņemt vērā DAS padomus, pārskatatbildības principa ietvaros ir ieteicams dokumentēt šo lēmumu un tā iemeslus, kā arī iesniegt šo dokumentāciju uzraudzības iestādēm revīzijas gadījumā.

## Kontaktpunkts

DAS ir galvenais kontaktpunkts gan uzraudzības iestādēm (VDAR 39.panta 1.punkta e) apakšpunkts), gan datu subjektiem (VDAR 38.panta 4.punkts) attiecībā uz jebkuru jautājumu, kas saistīts ar datu aizsardzību organizācijā. Tādēļ ir ļoti svarīgi pienācīgi sniegt DAS kontaktinformāciju uzraudzības iestādei un datu subjektiem. Turklāt prasība sniegt DAS kontaktinformāciju ir viens no pārredzamības principa elementiem saskaņā ar VDAR 12., 13. un 14.pantu.

VDAR neizslēdz, ka DAS izmanto iespēju konsultēties ar uzraudzības iestādēm par jebkuru jautājumu, kas saistīts ar datu aizsardzību organizācijā.

## Datu uzglabāšana

Lai gan pienākums reģistrēt apstrādes darbības ir paredzēts tikai datu pārziņiem un apstrādātājiem, nevis DAS, tomēr VDAR neaizliedz organizācijām uzticēt šo funkciju DAS. VDAR noteikts DAS **obligāto uzdevumu saraksts**, tādēļ organizācijām pēc saviem ieskatiem ir tiesības deleģēt jebkādus citus uzdevumus DAS. DG29 uzskata, ka šāda pienākuma nodošana DAS ir viens no instrumentiem, kas ļauj tam pildīt savus pienākumus, lai uzraudzītu atbilstību, informējot un konsultējot datu pārzini vai apstrādātāju[[15]](#endnote-15). Tā kā šis reģistrs ir efektīvs instruments pārskatatbildības nodrošināšanai, būtu pamatoti deleģēt šo pienākumu DAS.

# SECINĀJUMI UN PRAKTISKIE PADOMI

DAS ir viena no galvenajām personām, kas nodrošina atbilstību jaunajiem datu aizsardzības noteikumiem. DAS loma lielā mērā ir atkarīga no pašas attiecīgās organizācijas. Ja organizācija pienācīgi iesaistīs DAS visos ar datu aizsardzību saistītos jautājumos un nodrošinās nepieciešamos resursus, lai tas varētu veikt savas funkcijas, DAS varētu būt viens no noteicošajiem faktoriem, lai nodrošinātu atbilstību un veicinātu uzticēšanos sabiedrībā. Pretējā gadījumā DAS būs diezgan ilūziska figūra, kurai nav reālas funkcijas kā vien pārvaldīt ar datu aizsardzību saistīto saziņu, kas nav šī amata būtība saskaņā ar VDAR.

Pašvaldībām ir svarīgi iecelt kvalificētus DAS, kas, ņemot vērā sagatavoto personu trūkumu ES līmenī, varētu izrādīties sarežģīts uzdevums. Jebkurā gadījumā nākamie daži gadi noteiks, kā DAS loma attīstīsies. Sabiedrībai būtu pozitīvi, ja pašvaldības būtu viens no vadošajiem piemēriem attiecībā uz to, kā vislabāk izmantot DAS.

# ĀRĒJIE AVOTI UN TĪMEKĻA VIETNES

## Grāmatas

* **Harting, N.** Datenschutz-Grundverordnung: Das neue Datenschutzrecht in der betrieblichen Praxis, Verlag Dr. Otto Schmidt KG, Köln, 2016;
* **Voigt, P., von dem Bussche, A.** The EU General Data Protection Regulation (GDPR) – А Practical Guide, Springer International Publishing (2017);
* **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
* **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

## 29.panta darba grupas dokumenti

* DG29, Vadlīnijas par datu aizsardzības speciālistiem (DAS), WP 243;

## Tīmekļa saites

* <http://europa.eu/rapid/press-release_IP-18-386_lv.htm>
* <https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_lv>

# ATSAUCES

1. DG29, Vadlīnijas par datu aizsardzības speciālistiem (DAS), WP 243, 6.lpp. [↑](#endnote-ref-1)
2. Turpat [↑](#endnote-ref-2)
3. Turpat [↑](#endnote-ref-3)
4. Turpat, 6-7.lpp. [↑](#endnote-ref-4)
5. Turpat, 8.lpp. [↑](#endnote-ref-5)
6. Precīzu DG29 interpretāciju skatiet DG29, Vadlīnijas par datu aizsardzības speciālistiem (DAS), WP 243, 8.lpp. [↑](#endnote-ref-6)
7. Demmel, A. The New German Federal Data Protection Act, Squire Patton Boggs, URL: <<https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/09/the-new-german-federal-data-protection-act/27836--german-federal-data-protection-alert.pdf>> (26.03.2018); [↑](#endnote-ref-7)
8. DG29, Vadlīnijas par datu aizsardzības speciālistiem (DAS), WP 243, 12.lpp. [↑](#endnote-ref-8)
9. EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 58. [↑](#endnote-ref-9)
10. DG29, Vadlīnijas par datu aizsardzības speciālistiem (DAS), WP 243, 13.lpp. [↑](#endnote-ref-10)
11. Turpat, 14.lpp. [↑](#endnote-ref-11)
12. Vācija jau ieviesusi DAS aizsardzību pret atlaišanu, kā arī vienu gadu pēc amata izbeigšanas, izņemot ārkārtas izbeigšanas iemeslus. Skatiet Demmel, A. The New German Federal Data Protection Act, Squire Patton Boggs, URL: <<https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/09/the-new-german-federal-data-protection-act/27836--german-federal-data-protection-alert.pdf>> (26.03.2018); [↑](#endnote-ref-12)
13. DG29, Vadlīnijas par datu aizsardzības speciālistiem (DAS), WP 243, 15.lpp. [↑](#endnote-ref-13)
14. Turpat, 16.lpp. [↑](#endnote-ref-14)
15. DG29, Vadlīnijas par datu aizsardzības speciālistiem (DAS), WP 243, 17.lpp. [↑](#endnote-ref-15)