EIROPAS
KOMISIJA

Briselē, 25.4.2018.
SWD(2018) 125 final

**KOMISIJAS DIENESTU DARBA DOKUMENTS**

**Norādījumi par apmaiņu ar privātā sektora datiem Eiropas datu ekonomikā**

***Pavaddokuments dokumentam***

**Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai**

**"Ceļā uz vienotas datu telpas izveidi Eiropā"**

{COM(2018) 232 final}

## 1. Ievads

Uz datiem balstīta inovācija ir galvenais Eiropas izaugsmes un nodarbinātības veicinātājs. Galvenie tehniskie virzītājspēki ir internetā savākto datu svarīgums, aizvien pieaugošais to datu svarīgums, ko ģenerē lietu internetam (*Internet of Things — IoT*) pieslēgti objekti, aizvien pieaugošā lielo datu analīzes instrumentu pieejamība un atsevišķu mākslīgā intelekta lietotņu plašā pieejamība. Datu nekonkurējošais raksturs, kas dod iespēju vieniem un tiem pašiem datiem atbalstīt virkni jaunu produktu vai pakalpojumu vai jaunas ražošanas metodes, liecina, ka uzņēmumiem var būt lietderīgi apmainīties ar citiem uzņēmumiem ar vairāk to turējumā esošiem datiem, lai maksimāli varētu izmantot šo datu sniegto vērtīgo informāciju.

Jaunie, uz datiem balstītie darījumdarbības modeļi, kuru pamatā ir šie tehniskie virzītājspēki, ir iespēja ne tikai Eiropas lielajiem uzņēmumiem, bet arī mazajiem un vidējiem uzņēmumiem (MVU) un jaunuzņēmumiem. Tāpat arī valsts sektors sāk izmantot uz datiem balstītas inovācijas iespējas. Uzņēmumi jau gūst labumu no piekļuves valsts sektora informācijai, kas pieejama kā atvērtie dati1, kā arī no datu apmaiņas savā starpā. Tomēr MVU un jaunuzņēmumi joprojām saskaras ar šķēršļiem, kad dara pieejamus savus datus vai atkalizmanto citu uzņēmumu datus. Tas jo īpaši attiecas uz mašīnu ģenerētiem, nepersonizētiem datiem. Arī valsts sektora struktūrām ir jāmodernizē veids, kā tās funkcionē un izmanto jaunu datu avotu potenciālu, lai vairāk balstītos uz datiem un kļūtu rentablākas. Gaidāms, ka iedzīvotāji un uzņēmumi, jo īpaši MVU, gūs no tā labumu. Lai gan atsevišķos gadījumos attiecīgus uz datiem balstītus pakalpojumus var iegādāties tirgū, citos gadījumos valsts sektoram var būt nepieciešams tieši analizēt datus, kuru turētājs ir privāts uzņēmums, vai organizēt regulāru datu iegūšanu, piemēram, oficiālās statistikas vajadzībām. Šie dati varētu ne vienmēr būt pieejami valsts sektoram saistībā ar bažām par datu konfidencialitāti vai iespējamiem riskiem attiecībā uz uzņēmumu komerciālajām interesēm. Tas liek domāt, ka datu piegādes un (atkal)izmantošanas ("datu apmaiņas") jautājumi ir jārisina divās situācijās — uzņēmumu darījumos ar uzņēmumiem (*B2B*) un uzņēmumu darījumos ar valsts iestādēm / valsts sektoru (*B2G*).

Komisija ir jau ierosinājusi pasākumus, lai uzlabotu datu pieejamību uzņēmumiem. Ar Vispārīgo datu aizsardzības regulu (VDAR) un E-privātuma direktīvu2 Eiropas Savienībā (ES) ir ieviesta stabila sistēma personas datu un elektroniskās komunikācijas datu apstrādei, kura paredzēta, lai radītu digitālo uzticamību, kas ir galvenais priekšnoteikums jebkurai datu apmaiņai. Šī sistēma liek pamatus turpmākai konkurences priekšrocībai, lai Eiropas uzņēmēji iespējami labāk izmantotu datu tehnoloģijas. Turklāt priekšlikums regulai par nepersonizētu datu brīvu apriti3 atvieglos šādu datu pārsūtīšanu ES iekšienē.

---

1 Tostarp, izmantojot Eiropas Datu portālu: https://www.europeandataportal.eu/lv/homepage.

2 Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp.). Sk. arī priekšlikumu Eiropas Parlamenta un Padomes regulai par privātās dzīves neaizskaramību un personas datu aizsardzību elektroniskajā komunikācijā un ar ko atceļ Direktīvu 2002/58/EK (regula par privāto dzīvi un elektronisko komunikāciju) (COM(2017) 10 final, 10.1.2017.).

3 COM(2017) 495 final.

Komisija 2017. gada 10. janvāra paziņojumā "Veidojot Eiropas datu ekonomiku"4 ierosināja iespējamo datu piekļuves jautājumu pirmo izklāstu, jo īpaši attiecībā uz mašīnu ģenerētiem datiem un platformu darījumiem ar uzņēmumiem. Tā arī minēja to, cik svarīga sabiedrības interesēs ir piekļuve privātā sektora datiem.

Pamatojoties uz minēto paziņojumu, notika plašs dialogs ar ieinteresētajām personām. Tajā tika secināts, ka šajā posmā attiecīgais jautājums nedod pamatu horizontālam likumdošanas pasākumam un ka norādījumi būtu piemērotāki5.

Šim dienestu darba dokumentam pievienotajā paziņojumā6 Komisija definē vairākus galvenos principus, kas jāņem vērā, lai datu pārsūtīšana uzņēmumu darījumos ar uzņēmumiem un uzņēmumu darījumos ar valsts iestādēm būtu sekmīga visām iesaistītajām pusēm.

Turklāt šā dienestu darba dokumenta mērķis ir nodrošināt instrumentu kopumu uzņēmumiem, kas ir datu turētāji, datu izmantotāji vai vienlaikus gan datu turētāji, gan izmantotāji. Šajā nolūkā tajā iekļauti praktiski norādījumi par datu apmaiņas juridiskiem, darījumdarbības un tehniskiem aspektiem, kurus var izmantoti praksē, apsverot un sagatavojot datu pārsūtīšanu starp uzņēmumiem, kas nāk no tās pašas vai citas nozares.

Šajā dokumentā sniegtie norādījumi ir paredzēti visām ekonomikas nozarēm. Tā kā atsevišķu tirgu struktūras ir atšķirīgas, tās varētu būt jāpapildina ar konkrētai nozarei paredzētiem pasākumiem.

Visbeidzot, šis dokuments nerada jaunas tiesību normas un neskar Eiropas Savienības Tiesas (Tiesa) ES tiesību aktu interpretāciju. Tas nav saistošs Komisijai attiecībā uz ES tiesību aktu piemērošanu, jo īpaši attiecībā uz Līguma par Eiropas Savienības darbību (LESD) 101. un 102. pantā paredzētajiem konkurences noteikumiem.

4 COM(2017) 9 final.
5 https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-building-european-data-economy.
6 COM(2018) 232.

**2. Principi datu apmaiņai uzņēmumu darījumos ar uzņēmumiem (*B2B*) un uzņēmumu darījumos ar valsts iestādēm (*B2G*)**

Lai nodrošinātu **godīgus tirgus *IoT* objektiem, kā arī produktiem un pakalpojumiem, kas balstās uz datiem, kurus ir radījuši šādi objekti**, šim dienestu darba dokumentam pievienotajā paziņojumā7 ir definēti šādi principi:

a) **pārredzamība**. Attiecīgajās līgumattiecībās pārredzami un saprotami ir jānosaka i) personas vai struktūras, kam būs pieejami dati, kurus ģenerē produkts vai pakalpojums, šādu datu veids un detalizācijas pakāpe un ii) šādu datu izmantošanas mērķis;

b) **kopējas vērtības radīšana**. Attiecīgajās līgumattiecībās ir jāatzīst, ka, ja ģenerētie dati ir kāda produkta vai pakalpojuma izmantošanas blakusprodukts, šādu datu radīšanā ir iesaistītas vairākas puses;

c) **komerciālo interešu savstarpēja ievērošana**. Attiecīgajās līgumattiecībās ir jāpievēršas nepieciešamībai aizsargāt datu turētāju un datu izmantotāju komerciālās intereses un noslēpumus;

d) **neizkropļotas konkurences nodrošināšana**. Attiecīgajās līgumattiecībās ir jāpievēršas nepieciešamībai nodrošināt neizkropļotu konkurenci, kad notiek komerciāli jutīgu datu apmaiņa;

e) **datu iestrēgšanas iespēju samazināšana līdz minimumam**. Uzņēmumiem, kuri piedāvā produktu vai pakalpojumu, kas ģenerē datus kā blakusproduktu, ir jāatļauj pēc iespējas lielāka datu pārnesamība8. Attiecīgā gadījumā un atbilstīgi tirgus, kurā tie darbojas, īpašībām šiem uzņēmumiem ir arī jāapsver iespēja piedāvāt to pašu produktu vai pakalpojumu bez datu pārsūtīšanas vai tikai ar ierobežotu datu pārsūtīšanu starp produktiem vai pakalpojumiem, kuros ietverta šāda datu pārsūtīšana.

Paziņojumā arī teikts, ka turpmāk minēto principu ievērošana varētu palīdzēt **piegādāt valsts sektora struktūrām privātā sektora datus** ar preferenciāliem atkalizmantošanas nosacījumiem:

a) **privātā sektora datu izmantošanas samērīgums.** Pieprasījumiem par privātā sektora datu piegādi ar preferenciāliem atkalizmantošanas nosacījumiem ir jābūt pamatotiem ar skaidrām un pierādāmām sabiedrības interesēm. Privātā sektora datu pieprasījumam ir jābūt saprātīgam un saistītam ar sabiedrības interesēm, kā arī samērīgam detalizētības, nozīmības un datu aizsardzības ziņā. Privātā sektora datu piegādes un atkalizmantošanas izmaksām un pūliņiem ir jābūt samērīgiem salīdzinājumā ar paredzamajiem sabiedrības ieguvumiem;

b) **nolūku ierobežošana**. Privātā sektora datu izmantošanai ir jābūt skaidri ierobežotai līdz vienam vai vairākiem nolūkiem, kuri ir jānorāda pēc iespējas skaidrāk uzņēmuma un

7 COM(2018) 232.

8 Piemēram, tie var būt dati, ko ģenerējuši roboti rūpnieciskajos procesos un kas ir būtiski pēcpārdošanas pakalpojumu (piemēram, remonta un apkopes) sniegšanā, vai dati par pakalpojumu sniedzēju vērtējumu.

valsts iestādes sadarbības līguma noteikumos. Tajos var būt ietverts šo datu izmantošanas ilguma ierobežojums. Privātā sektora uzņēmumam ir jāgūst īpaša pārliecība, ka iegūtie dati netiks izmantoti nesaistītās administratīvās vai tiesiskās procedūrās. Šajā saistībā modelis varētu būt stingrie juridiskie un ētiskie noteikumi attiecībā uz statistikas konfidencialitāti Eiropas Statistikas sistēmā;

c) **"nekaitēt".** Uzņēmumu un valsts iestāžu sadarbībai datu jomā ir jānodrošina, ka tiek ievērotas leģitīmās intereses, galvenokārt tirdzniecības noslēpumu un citas komerciāli jutīgas informācijas aizsardzība. Uzņēmumu un valsts iestāžu sadarbībai datu jomā ir jāļauj uzņēmumiem turpināt pārvērst naudā no attiecīgajiem datiem gūtos labumus attiecībā pret citām ieinteresētajām personām;

d) **datu atkalizmantošanas nosacījumi.** Uzņēmumu un valsts iestāžu sadarbības līgumiem datu jomā ir jābūt savstarpēji izdevīgiem, vienlaikus atzīstot sabiedrības interešu mērķi, piešķirot valsts sektora struktūrai preferenciālu režīmu salīdzinājumā ar citiem klientiem.

Tam jo īpaši jāatspoguļojas saistībā ar vienošanos par kompensāciju, kuras apmēru var salāgot ar attiecīgo sabiedrības interešu mērķi.

Pret uzņēmumu un valsts iestāžu sadarbības līgumiem datu jomā, kuros piedalās vienas un tās pašas iestādes, kuras pilda vienas un tās pašas funkcijas, ir jāizturas nediskriminējoši.

Uzņēmumu un valsts iestāžu sadarbības līgumiem datu jomā ir jāsamazina nepieciešamība vākt datus, piemēram, aptaujās. Tam ir jāsamazina kopējais slogs iedzīvotājiem un uzņēmumiem;

e) **mazināt privātā sektora datu ierobežojumus.** Lai novērstu iespējamos privātā sektora datu ierobežojumus, tostarp neobjektivitāti, uzņēmumiem, kuri piegādā datus, ir jāpiedāvā saprātīgs un samērīgs atbalsts, lai palīdzētu novērtēt norādītājiem mērķiem nepieciešamo datu kvalitāti, tostarp attiecīgā gadījumā ar iespēju veikt revīziju vai citādi pārbaudīt datus. Uzņēmumiem nedrīkst pieprasīt uzlabot attiecīgo datu kvalitāti. Savukārt valsts struktūrām ir jānodrošina, ka dati no dažādiem avotiem tiek apstrādāti tā, lai nepieļautu iespējamu "atlases neobjektivitāti";

f) **pārredzamība un sabiedrības līdzdalība.** Uzņēmumu sadarbībai ar valsts iestādēm ir jābūt pārredzamai līguma pušu un to mērķu ziņā. Ir jāpublisko valsts struktūru nodomi un uzņēmumu sadarbības ar valsts iestādēm paraugprakse, ja vien tas neapdraud datu konfidencialitāti.

## 3. Datu apmaiņa uzņēmumu darījumos ar uzņēmumiem (*B2B*) — praktiski norādījumi

Datu piegāde un atkalizmantošana *B2B* darījumos var notikt dažādos veidos to tehnisko mehānismu ziņā, kuri ir pamatā darījumdarbības modeļiem un juridiskajam instrumentam, kas atbalsta *B2B* datu apmaiņas kārtību. Šajā iedaļā daži no tiem ir aprakstīti sīkāk.

### 3.1. *B2B* datu apmaiņas modeļi

Datu apmaiņas pamatā esošie darījumdarbības modeļi var diezgan būtiski atšķirties, un tas lielā mērā ir atkarīgs no attiecīgo datu veida un stratēģiskajām uzņēmumu interesēm. Tie var ietvert gan atvērto datu pieeju, gan īpašas datu partnerības tikai ar vienu personu:

a) **atvērto datu pieeja**. Atvērto datu pieeja, atbilstīgi kurai datu piegādātājs dara pieejamus attiecīgos datus principā atvērtam (atkal)izmantotāju lokam, paredzot pēc iespējas mazāk ierobežojumu un nosakot vai nu ļoti mazu atlīdzību vai nenosakot to vispār, var tikt izraudzīta, ja datu piegādātājs ir ļoti ieinteresēts datu atkalizmantošanā. Kā piemērus var minēt pakalpojumu sniedzējus, kas, lai sasniegtu galalietotājus, vēlas izmantot trešo personu lietotņu izstrādātāju ekosistēmu;

b) **datu monetizācija datu tirgū**. Datu monetizācija vai tirdzniecība var notikt datu tirgū kā starpniecības darbība, pamatojoties uz divpusējiem līgumiem un saņemot par to atlīdzību. Tas var ieinteresēt uzņēmumus, kuri nezina iespējamos savu datu atkalizmantotājus un kuru mērķis ir īstenot vienreizējus datu monetizācijas centienus. Šis mehānisms šķiet piemērots, ja 1) pastāv nelieli riski saistībā ar attiecīgo datu nelikumīgu izmantošanu, 2) datu piegādātājam ir pamats uzticēties (atkal)izmantotājam vai 3) datu piegādātājam ir tehniski mehānismi, ar ko novērst vai atklāt nelikumīgu izmantošanu. Parauglīguma noteikumi var samazināt datu izmantošanas līgumu sagatavošanas izmaksas;

c) **datu apmaiņa slēgtā platformā**. Datu apmaiņa var notikt slēgtā platformā, ko izveidojis viens galvenais datu apmaiņas vides dalībnieks vai neatkarīgs starpnieks. Šajā gadījumā dati var tikt piegādāti pret finansiālu atlīdzību vai pret pakalpojumiem ar pievienoto vērtību, kurus sniedz, piemēram, pašā platformā. Šis risinājums ļauj sniegt pakalpojumus ar pievienoto vērtību un tādējādi nodrošina visaptverošu risinājumu stabilākām datu partnerībām un vairāk kontroles mehānismu datu izmantošanas jomā; parauglīguma noteikumi var samazināt datu izmantošanas līgumu sagatavošanas izmaksas. Ja datu apmaiņa ir ekskluzīva, tai būtu jāatbilst konkurences noteikumiem[9].

Ir iespējamas šo modeļu variācijas un kombinācijas, kuras jāpielāgo katra konkrēta uzņēmuma vajadzībām. Terminu "datu apmaiņa" lieto, lai aprakstītu visus iespējamos veidus un modeļus, kas ir pamatā *B2B* datu piekļuvei vai pārsūtīšanai.

9 Sk., piemēram, Komisijas Pamatnostādnes vertikālo ierobežojumu jomā (OV C 130, 19.05.2010., 1. lpp.) un Norādījumus par Komisijas prioritātēm, piemērojot EK līguma 82. pantu [tagad LESD 102. pants] dominējošu uzņēmumu ļaunprātīgai, izslēdzošai rīcībai (OV C 45, 24.2.2009., 7. lpp.).

### 3.2. Datu apmaiņas juridiskie aspekti — datu izmantošanas vai licences līgumi

*B2B* datu apmaiņu parasti īsteno, pamatojoties uz līgumiem. Datu izmantošanas vai licences līgumu puses vienojas par līguma priekšmetu un vērtību, kā arī par visiem pārējiem līgumā paredzētajiem nosacījumiem. Datu monetizācijas līgumi pēc būtības var būt ne tikai divpusēji, bet arī noslēgti starp vairākām personām.

Īpaša uzmanība jāpievērš atbilstīgu datu izmantošanas vai licences līgumu noteikumu izstrādei, lai abi līgumu veidi atbilstu spēkā esošajiem tiesību aktiem, jo īpaši tiem tiesību aktiem, kas var novērst datu apmaiņu vai piemērot tai īpašus nosacījumus, un nodrošinātu, ka tiek saglabātas katras puses stratēģiskās intereses un konkurence.

Jau tiek izstrādāti parauglīguma noteikumi dažādiem datu apmaiņas līgumiem un atsevišķām nozarēm vai datu apmaiņas veidiem. Komisija ar Datu apmaiņas atbalsta centra palīdzību, kurš sāks darboties 2019. gada sākumā, plāno apkopot paraugpraksi, spēkā esošos parauglīguma noteikumus un kontrollapas10.

Datu izmantošanas līgumu sagatavošanā un/vai apspriešanā uzņēmumiem var palīdzēt šādi apsvērumi:

a) Kādi dati tiks darīti pieejami?

- Aprakstiet datus, ar kuriem vēlaties apmainīties pēc iespējas konkrētāk un precīzāk (piemēram, pētniecības un izstrādes dati, klientu dati, diagnostikas dati), tostarp turpmāk sagaidāmo atjauninājumu līmeņus. Ja kopā ar datu kopām notiek apmaiņa ar skaidrojošiem resursiem, kas ļauj veikt analīzi (piemēram, metodēm, modeļiem), tie ir jāapraksta.
- Kādus kvalitātes līmeņus var nodrošināt šiem datiem (arī laika gaitā)? Sniegtajiem datiem jābūt kvalitatīviem, t. i., precīziem, ticamiem un, vajadzības gadījumā, atjauninātiem. Nodrošiniet, lai dati nebūtu pazuduši, dublēti, nestrukturēti. Norādiet datu avotu/izcelsmi un to, kā tie tika savākti/veidoti. Var izveidot mehānismu, kas paredzēts, lai ziņotu par kļūdām datos.
- Vai datu apmaiņa ir saistīta ar datu kopu vai datu plūsmu?
- Nodrošiniet atbilstību juridiskajām saistībām, kas var liegt piekļuvi attiecīgajiem datiem vai to pārsūtīšanu citiem. Nodrošiniet to tiesību ievērošanu, kas citiem var būt uz šiem datiem. Pārbaudiet tiesības uz datos ietverto saturu (intelektuālā un rūpnieciskā īpašuma tiesības).
- Nodrošiniet datu aizsardzības tiesību aktu ievērošanu. Cita starpā pārbaudiet, vai saskaņā ar Vispārīgo datu aizsardzības regulu pastāv juridisks pamats personas datu apstrādei.

10 Sk. pielikumu Komisijas Īstenošanas lēmumam par 2018. gada darba programmas pieņemšanu un Eiropas infrastruktūras savienošanas instrumenta (EISI) — telekomunikāciju nozare — finansēšanu, 42. lpp.

b) Kas var piekļūt attiecīgajiem datiem un tos (atkal)izmantot?

   – Nodrošiniet, lai līgumā būtu pārredzami, skaidri un saprotami definēts, kam ir tiesības piekļūt datiem, tiesības tos (atkal)izmantot un tiesības tos izplatīt un saskaņā ar kādiem nosacījumiem. Norādiet, vai un kā datus var licencēt atkalizmantošanai. Sīki izskaidrojiet licenču nosacījumus par datu atkalizmantošanu un izplatīšanu. Jāņem vērā arī apakšlicencēšanas vajadzības — vai nu tā ir īpaši jāizslēdz vai jāprecizē nosacījumi, atbilstīgi kuriem tā ir atļauta un kādiem datu veidiem.

   – Tiesībām piekļūt datiem un tos (atkal)izmantot nav jābūt neierobežotām. Līgums var ierobežot piekļuves tiesības, piemēram, tikai konkrētu profesionālo grupu pārstāvjiem (piemēram, lauksaimniekiem) vai saistīt tās ar noteiktiem datu izmantošanas mērķiem (piemēram, ierobežotu izmantošanu komerciālos nolūkos).

c) Ko (atkal)izmantotājs var darīt ar datiem?

   – Sarunās par līgumu (atkal)izmantotājam jābūt pēc iespējas atklātākam un skaidrākam jautājumā par to, kā šie dati tiks izmantoti, tostarp kā tos izmantos pakārtotās personas. Tas nodrošinās pārredzamību un palielinās datu piegādātāja uzticamību.

   – Norādiet datu precīzu izmantošanas veidu, tostarp tiesības uz šo datu atvasinājumiem (analīzi).

   – Definējiet pakārtotām personām noteikumus par datu neizpaušanu.

d) Definējiet tehniskos līdzekļus datu piekļuvei un/vai apmaiņai, tostarp

   – datu piekļuves biežumu un ielāžu maksimālo skaitu;

   – IT drošības prasības;

   – pakalpojumu līmeņus atbalstam.

e) Kādi dati ir jāaizsargā, un kā tie tiek aizsargāti?

   – Nodrošiniet, lai būtu ieviesti atbilstīgi pasākumi datu aizsardzībai. Šie pasākumi jāpiemēro datu apmaiņas darījumiem un datu uzglabāšanai, jo datus var nozagt vai ļaunprātīgi izmantot organizētās noziedzības grupējumi un individuāli hakeri. Datus var izplatīt arī nejauši, piemēram, cilvēka kļūdas vai tehniskas problēmas dēļ. Datiem var arī piekļūt nesankcionēti, tos var izpaust vai arī nozaudēt.

   – Nodrošiniet tirdzniecības noslēpumu, komerciāli jutīgas informācijas, licenču, patentu, intelektuālā īpašuma tiesību aizsardzību. Sakarā ar datu apmaiņu nevienas personas mērķis nedrīkstēs būt jutīgas informācijas ieguve no otras personas.

f) Ietveriet atbildības noteikumus par kļūdainu datu piegādi, pārtraukumiem datu pārraidē, nekvalitatīvu skaidrojošo darbu, ja tas tiek izplatīts kopā ar datu kopām, vai datu iznīcināšanu/nozaudēšanu vai izmainīšanu (ja tā ir nelikumīga vai nejauša), kas potenciāli var radīt zaudējumus.

g) Definējiet abu pušu tiesības veikt revīzijas savstarpējo saistību izpildes jomā.

h) Kāds ir paredzētais līguma darbības termiņš? Kam ir tiesības pārtraukt līgumu? Kāds paziņojums jāsniedz partneriem?

i) Vienojieties par piemērojamajiem tiesību aktiem un strīdu izšķiršanas mehānismiem.

### 3.3. Datu apmaiņas tehniskie aspekti

Ir vairāki tehniskie mehānismi datu apmaiņai *B2B* kontekstā. Daži tehniskie mehānismi var nodrošināt datu izmantošanas noteikumus, vienlaikus piedāvājot uzticamu un drošu vidi datu kopu apmaiņai11.

Var izšķirt trīs veidu mehānismus: a) datu turētājs atlasītos datus dara tieši pieejamus lielākam skaitam atkalizmantotāju, piemēram, izmantojot lietojumprogrammas saskarni; b) datu turētājs, izmantojot starpnieku (datu tirgu), dara pieejamus atlasītos datus vienam vai vairākiem atkalizmantotājiem, paredzot ierobežotu kontroli pār turpmāko izmantošanu; c) datu turētājs, izmantojot starpnieku (datu telpu vai platformu), dara pieejamus atlasītos datus vienam vai vairākiem atkalizmantotājiem tādā vidē, kas ļauj stingrāk kontrolēt un izsekot turpmāko izmantošanu.

a) **Datu apmaiņa "no viena pie daudziem", izmantojot lietojumprogrammas saskarni (*Application Programming Interface* — *API*) vai rūpniecības datu platformu**. Atsevišķi uzņēmumi, kas ir iesaistījušies datu pārsūtīšanā citiem, izmanto vienpusējus mehānismus, kas tehniski nodrošina piekļuvi datiem, piemēram, *API* vai īpašas platformas, kuras tie ir izveidojuši datu uzglabāšanai, apstrādei un apmaiņai.

   Arvien izplatītāka kļūst datu piekļuves atvēršana trešām personām, izmantojot publiskas *API*, t. i., *API*, kas pieejamas plašākai sabiedrībai, nevis tikai personām tajā pašā organizācijā. *API* skaits kopš 2010. gada ir būtiski pieaudzis un turpina pieaugt12.

   *API* var atvieglot jo īpaši maziem uzņēmumiem darījumdarbības datu izmantošanu vai atkalizmantošanu. Vienkāršas lietošanā un labi izstrādātas *API* palīdz izveidot un paplašināt ekosistēmas ar jauniem un inovatīviem produktiem, izmantojot jau savāktos datus.

   *API* ir potenciāls veicināt sadarbspēju, ļaujot lietojumprogrammatūrām veikt datu kopu un datu plūsmu apmaiņu13. Būtībā *API* var ietvert pašu datu kopu specifikācijas un nodrošināt tehniskā līmenī piekļuves tiesību pārvaldību.

11 Aprakstītie mehānismi un piemēri ir ņemti no pētījuma par datu apmaiņu starp uzņēmumiem Eiropā, ko Komisijas uzdevumā veica uzņēmums *Everis* (drīzumā būs pieejams pētījuma ziņojums).
12 http://www.programmableweb.com/api-research.
13 Sk. sīkāku informāciju par norādījumu dokumentu *API* jomā, kuru izstrādāja tīkls *Share PSI* un Konkurētspējas un inovāciju pamatprogrammas ietvaros līdzfinansēja Eiropas Komisija: http://www.w3.org/TR/dwbp/#useanAPI.

Pamatojoties uz iepriekš minēto, Komisija mudina14 uzņēmumus visā Eiropā apsvērt iespēju daudz plašāk izmantot atvērtas, standartizētas un labi dokumentētas *API*. Šā procesa ietvaros varētu apsvērt arī jautājumu par to, kā nodrošināt datu pieejamību mašīnlasāmos formātos un saistītos metadatus.

***TomTom*** ir Nīderlandes uzņēmums, kas ražo satiksmes, navigācijas un kartēšanas produktus. Saskaņā ar konstatējumiem, kas izdarīti Komisijas finansētajā pētījumā15, lielākā daļa ieņēmumu no uzņēmuma darbības nāk no datiem (kartēm un tiešsaistes pakalpojumiem), kas tiek licencēti citiem uzņēmumiem.

*TomTom* piedāvā izstrādātājiem lietojumprogrammu saskarnes16 kā datu piekļuves līdzekli.

Saskaņā ar uzņēmuma *TomTom* teikto tam salīdzinājumā ar citiem datu apmaiņas tehniskajiem līdzekļiem ir šādas priekšrocības:

- ērta un ātra piekļuve datiem,
- datu izmantošanas uzraudzība,
- līguma pārkāpumu pārbaude,
- ātra rīcība gadījumos, kad dati tiek izmantoti ļaunprātīgi (t. i., datu piekļuves izbeigšana vai pārtraukšana).

Uzņēmumi, jo īpaši lielāki uzņēmumi, izstrādā arī īpašas **datu platformas**, lai pārvaldītu regulāru datu pārsūtīšanu trešām personām. Tie piedāvā papildu funkcijas attiecībā uz datu apmaiņu, jo īpaši attiecībā uz datu divpusēju apmaiņu, uzglabāšanu platformā un papildu pakalpojumiem, kas sniedzami papildus datiem (pamatojoties uz datu analīzi).

***Airbus*** ir Eiropas daudznacionāla korporācija, kas izstrādā, izgatavo un pārdod civilās un militārās aeronavigācijas produktus.

Izmantojot dažādus veidus, lai padarītu datus pieejamus iestādēm un darījumdarbības partneriem, 2017. gada jūnijā uzņēmums *Airbus* aktivizēja *Skywise*17 — "atvērto digitālo platformu aviācijai".

Klientu uzņēmumi padara datus pieejamus apmaiņā pret pakalpojumiem, kuru pamatā ir datu analīze.

Pamatojoties uz *Hadoop* programmatūru, šīs tehniskās pieejas galvenā priekšrocība ir nevainojama integrācija ar aviosabiedrību pašreizējo IT infrastruktūru, tādējādi palīdzot dalībniekiem padarīt savus datus pieejamus platformā. *Airbus* var strādāt, pamatojoties uz sākotnējo faila formātu, un ar platformas starpniecību atsūtīt atpakaļ analīzes rezultātus, izmantojot kopīgas tabulas un vizualizācijas instrumentus.

14 COM(2017) 9 final.
15 *Everis, Study on data-sharing between companies in Europe* (drīzumā būs pieejams).
16 https://developer.tomtom.com/tomtom-maps-apis-developers.
17 https://services.airbus.com/maintenance/expertise-and-other-services/skywise/skywise.

b) **Datu monetizācija, izmantojot datu tirgu "no daudziem pie daudziem"**. Terminu "datu tirgus" šajā dokumentā izmanto, lai apzīmētu konkrēta veida starpnieku, kam var būt trīs galvenās funkcijas: 1) kontaktu dibināšana starp potenciālajiem datu piegādātājiem un datu pircējiem; tas var ietvert konkrētus iestatījumus, pateicoties kuriem datu pārsūtīšanas sagatavošanas pirmajā daļā potenciālais datu piegādātājs un potenciālais pircējs var palikt anonīmi, jo jau piegādes vai pirkšanas iecere var atklāt neizpaužamu darījumdarbības informāciju (turpmākās darījumdarbības stratēģijas); 2) faktiskā datu (un saskaņotās kompensācijas) pārsūtīšana, proti, uzticamības radīšana, ka sarunu gaitā sarunu objekts netiks mainīts; 3) apliecināšanas (ka darījums ir faktiski noticis) funkcija, kura ir potenciāli interesanta saistībā ar uzrādīšanu uzņēmuma bilancē. Turklāt šādi starpnieki var sniegt papildu pakalpojumus, piemēram, parauglīguma punktu izstrādes vai anonimizācijas pakalpojumus (ja apmaiņa notiek ar personas vai konfidenciāliem datiem). Šā veida starpnieka funkcijas beidzas, tiklīdz ir pārsūtīti dati.

***DAWEX***18 ir 2015. gadā dibināts Francijas uzņēmums, kas sevi raksturo kā "globālu datu tirgu".

*DAWEX* nepērk un nepārdod datus. Tā vietā *DAWEX* apvieno uzņēmumus, kas ir ieinteresēti datu monetizācijā un atkalizmantošanā, un veicina pārredzamību starp datu piegādātājiem un izmantotājiem, nodrošinot, ka tie sazinās un veic darījumus tieši platformā.

*DAWEX* izstrādāja vairākus instrumentus, lai palīdzētu gan datu piegādātājiem, gan izmantotājiem saprast, novērtēt datus un informēt par tiem. Vizualizācijas instrumenti (piemēram, intensitātes kartes, sistemātiskās kartes) nodrošina datu izmantotājiem dažādu informāciju par pilnīgu datu kopu, ar kuru var droši apmainīties pirms darījuma pabeigšanas. Lai izvairītos no jebkādas neobjektivitātes, izlases veidošanas instrumenti automātiski ģenerē reprezentatīvas datu izlases, pamatojoties uz algoritmiem. Datu izmantotāji un datu piegādātāji sazinās, izmantojot platformā iestrādātu ziņapmaiņas rīku. Turklāt *DAWEX* atbalsta līgumattiecību sarunas, nodrošinot automātiski ģenerējamus paraugnoteikumus.

18 https://www.dawex.com/en/.

c) **Datu apmaiņa, izmantojot tehnisko iespējotāju**. Atšķirībā no iepriekš aplūkotā starpnieku veida šādi tehniskie iespējotāji papildus datu apmaiņai ir īpaši orientēti uz pakalpojumu sniegšanu, piemēram, attiecīgo datu apstrādi, lai reaģētu uz konkrētām uzņēmuma vajadzībām vai jautājumiem. Svarīgākais ir tas, ka šāda veida starpnieks varētu nodrošināt papildu funkcijas, kas ļautu datu piegādātājam kontrolēt datu izmantošanu, jo īpaši datu pārsūtīšanas līguma noteikumu ievērošanu. Tas var ietvert datu izmantojuma izsekošanas un identificēšanas veidus, piemēram, visu datu piekļuves un apstrādes darbību reģistrēšanu — potenciāli izmantojot sadalītās virsgrāmatas tehnoloģiju (blokķēdi) — vai digitālo ūdenszīmju iespiešanas veidu izstrādi. Starpnieks var izstrādāt arī pašregulācijas gadījumus datu telpas vai platformas izmantotāju kopienā, iespējams, ietverot sankciju kopumu datu izmantotājiem, kas pārkāpj individuālus datu pārsūtīšanas līgumus.

***Nallian*19** ir izstrādājis mākonī izvietotu platformu, kas dod iespēju apmainīties ar reāllaika datiem un atbalsta procesa sinhronizāciju. Uzņēmums strādā ar pamata datu apmaiņas tehnoloģijas slāni, kuru var pielāgot, lai tas apmierinātu kādas konkrētas kopienas vai domēna datu izmantotāju vajadzības. Platformas pamatā ir mākoņtehnoloģija apvienojumā ar kopienas pārvaldības instrumentu.

Pašreizējie *Nallian* tehniskā risinājuma izmantotāji ir uzņēmumi, kas darbojas loģistikā, vertikālās piegādes ķēdēs un multimodālo pārvadājumu tīklos. Šiem uzņēmumiem ļoti svarīga ir spēja atrisināt sadrumstalotības jautājumus un apmainīties ar datiem bez pārtraukumiem un traucējumiem.

Šī platforma pieļauj dažādus datu ievades variantus mākonī — gan vienkāršas failu augšupielādes, gan uz *API* balstītus integrācijas veidus. Platformu papildina *API* ar pievienoto vērtību un lietotnes, kas izmanto kopīgu datu modeli, lai gūtu labumu no visiem platformā uzglabātajiem datiem un nodrošinātu izmantotājiem vērtīgus analīzes rezultātus. Visbeidzot, platforma pieļauj arī datus, kas piegādāti, izmantojot pievienotas ierīces, vai *B2B* ziņojumus, ar kuriem apmainās, izmantojot elektronisko datu apmaiņu (*electronic data interchange — EDI*).

Platforma ļauj datu piegādātājiem saglabāt detalizētu kontroli, lai tie zinātu, kam ir piekļuve, kuriem datiem un kādam nolūkam. Šī kontrole ir iespējota ar platformā iestrādātu tiesību piešķiršanas programmu, kas ļauj datu piegādātājiem definēt funkcijas un apmaiņas noteikumus dažādajiem kopienas dalībniekiem līdz pat lauka līmenim, tostarp lietotņu nodrošinātājiem. Turklāt platforma atvieglo datu anonimizāciju un apkopošanu, lai izpildītu vajadzīgās privātuma prasības.

19 https://www.nallian.com/.

## 4. *B2G* sadarbības datu jomā sekmīga īstenošana — praktiska kontrollapa

Datu piegāde un atkalizmantošana *B2G* darījumos var notikt dažādos veidos gan pamatā esošo mehānismu, gan tos atbalstošā juridiskā instrumenta ziņā. Šajā iedaļā daži no tiem ir aprakstīti sīkāk.

### 4.1. *B2G* datu apmaiņas modeļi

a) **Datu ziedošana**. *B2G* datu piegāde varētu tikt veikta kā datu ziedošana. To var uzskatīt par korporatīvās sociālās atbildības veidu. Viens no iespējamajiem rezultātiem varētu būt tāds, ka šādu datu ziedošanas programmu atbalstītu specializēta grupa, kas palīdzētu visām personām, kuras, iespējams, būtu ieinteresētas datu izmantošanā.

> ***Mastercard* datu filantropija**20
>
> *Mastercard* uzskata, ka organizācijām, kuru misija ir cilvēku ciešanu mazināšana, — neatkarīgi no to lieluma un ietekmes — jābūt vajadzīgajiem instrumentiem un resursiem, lai piekļūtu datiem un izmantotu tos problēmu atrisināšanai. *Mastercard* Iekļaujošas izaugsmes centrs ir apņēmies novērst nepilnības ar datu filantropijas palīdzību:
> - veicot datu apmaiņu, piemēram, piešķirot piekļuvi saviem īpašumtiesību datiem — veidā, kas pilnībā aizsargā patērētāju privātumu —, lai palīdzētu pētniecībai;
> - veicot apmaiņu ar zināšanām par datiem, piemēram, piesaistot iekšējos ekspertus, lai sagatavotu analīzi un publiskotu konstatējumus plašākai lietošanai;
> - piesaistot ekspertus, piemēram, sadarbojoties ar saviem partneriem, lai nodrošinātu papildu zināšanas un spējas.

b) **Balvas**. *B2G* sadarbībā var tikt paredzētas arī balvas, kas mudinātu privātpersonas un uzņēmumus, kuri specializējušies datu analīzē, rast risinājumus konkrētām, sabiedrības interesi izraisošām problēmām. Piemēram, sabiedriska organizācija varētu izvirzīt problēmu sadarbībā ar uzņēmumu, kas nodrošinātu privātā sektora datus, kuri vajadzīgi šīs problēmas atrisināšanai.

> **"*Horizon*" balva lielo datu tehnoloģiju jomā**21
>
> ES finansējuma programmas "Apvārsnis 2020" ietvaros lielo datu tehnoloģiju jomā tika izsludināta balva par to, lai rastu veidus, kā ar precīzākas prognozēšanas sistēmas palīdzību optimizēt energotīklu izmantošanu. Uzvarētājrisinājumiem būs jāpierāda spēja analizēt ļoti lielus strukturētu ģeotelpisko temporālo datu kopu krājumus, laikapstākļu laika ierakstus un citus datus ar dažādiem parametriem, ko izmanto energotīkla darbības pārvaldībā.

20 https://mastercardcenter.org/action/call-action-data-philanthropy/.
21 http://ec.europa.eu/research/horizonprize/index.cfm?prize=bigdata.

c) ***B2G* datu partnerības.** *B2G* sadarbība var notikt kā datu partnerības. Valsts sektora struktūras ar privātiem uzņēmumiem var noslēgt līgumus, kuros ietverta savstarpēja datu apmaiņa atbilstīgi PSI direktīvai22 attiecībā uz valsts sektora informācijas apmaiņu ar privāto sektoru. Tas var radīt ieguvumus arī privātajam uzņēmumam, jo tas varēs izmantot privātā un valsts sektora datu korelācijas analīzes rezultātus.

**Mobilo tālruņu datu kvalitātes novērtēšana kā statistikas avots — Beļģijas statistikas aģentūras un *Eurostat* pētījums**23

Beļģijas statistikas aģentūras un *Eurostat* kopīgi veiktais pētījums atklāja mobilo tīklu datu potenciālu iedzīvotāju blīvuma novērtēšanā. Tā mērķis bija novērtēt Beļģijas mobilo tālruņu datu (kas iegūti no galvenā tīkla operatora *Proximus*) kvalitāti, īpašu uzmanību pievēršot faktiskajam pašreizējam iedzīvotāju skaitam. Mobilo tīklu dati tika testēti attiecībā uz iekšējo konsekvenci un salīdzināti ar Beļģijas 2011. gada tautas skaitīšanas rezultātiem, kas pastāvīgi tiek atjaunināti kā daļa no iedzīvotāju reģistra. Privātuma apsvērumu dēļ abas datu kopas tika apkopotas24.
Pētījuma rezultāti bija lietderīgi abām pusēm. No vienas puses, varēja pierādīt, ka mobilo tīklu dati sniedz ticamu un precīzu informāciju, ar kuru var papildināt tradicionālo statistiku. No otras puses, mobilo tīklu operatori varēja, piemēram, izmantot pastāvīgo iedzīvotāju datus, lai uzlabotu aplēses par personu mobilitāti tādu jaunu lietotņu izstrādei, kuras nodrošina mobilā tīkla operators.

d) **Starpnieki**. Gadījumos, kad uzņēmums un valsts sektora struktūra iepriekš nav sadarbojušies un abu starpā nav uzticības, iegūt analīzes rezultātus, kas nepieciešami sabiedrības interešu labā, var uzdot starpniekam.

**Patērētāju datu izpētes centrs (*Consumer Data Research Centre* — *CDCR* (Apvienotā Karaliste))**25

Katru dienu tiek iegūts liels daudzums Apvienotās Karalistes patērētāju datu, kas nodrošina vērtīgus analīzes rezultātus, lai palīdzētu uzņēmumiem strādāt efektīvāk. *CDRC* mērķis ir strādāt ar organizācijām, lai darītu pieejamus to datus uzticamiem pētniekiem un tie tādējādi varētu piedāvāt risinājumus, kas veicina ekonomikas izaugsmi un uzlabo sabiedrības labklājību.

22 Eiropas Parlamenta un Padomes Direktīva 2003/98/EK par valsts sektora informācijas atkalizmantošanu (OV L 345, 31.12.2003., 90. lpp.).
23 *De Meersman* un citi (2016), "*Assessing the Quality of Mobile Phone Data as a Source of Statistics*", https://ec.europa.eu/eurostat/cros/system/files/assessing_the_quality_of_mobile_phone_data_as_a_source_of_statistics_q2016.pdf.
24 Statistikas biroji uztur reģistrus, kas satur personu un uzņēmumu datus, taču šos reģistrus nevar nodot citām personām sakarā ar personas datu aizsardzību un statistikas konfidencialitātes ierobežojumiem. Tomēr privātā sektora dati var būt saistīti ar reģistru datiem, vienlaikus nodrošinot datu drošību. Apkopotos statistikas rezultātus, kurus nevar izsekot līdz datu subjektam, var publicēt, pamatojoties uz šo analīzi.
25 https://www.cdrc.ac.uk/.

e) **"Pilsonisko datu apmaiņa".** Privātpersonas var tikt mudinātas atļaut valsts sektora struktūrām apstrādāt viņu personas datus, kurus iepriekš apstrādāja privāts uzņēmums. Jāuzsver, ka šajā gadījumā valsts iestādēm arī jāievēro datu aizsardzības tiesību akti. Apstrādei jābūt saskaņā ar atbilstīgu juridisko pamatu (piemēram, piekrišanai jāatbilst 6. panta 1. punkta a) apakšpunktam vai sabiedrības interesēs veiktu uzdevumu izpildei jāatbilst 6. panta 1. punkta e) apakšpunktam26). Šāda "pilsonisko datu apmaiņa", visticamāk, darbotos situācijās, kurās ir vai nu pietiekami spēcīga saikne starp iedzīvotājiem un attiecīgo valsts sektora struktūru (piemēram, pašvaldību, kur viņi dzīvo), vai sabiedrības interešu mērķis ir īpaši pārliecinošs, raugoties no iedzīvotāju viedokļa (konkrētu slimību apkarošana, ceļotāju plūsmu novirzīšana uz populāriem pasākumiem utt.).

### 4.2. Juridiskie un praktiskie apsvērumi *B2G* datu apmaiņas sadarbības jomā

Datu izmantošanas līgumu sagatavošanā un/vai apspriešanā valsts struktūrām un uzņēmumiem var palīdzēt šādi apsvērumi:

a) valsts struktūrām jānosaka sabiedrības interešu mērķis, privātā sektora dati un vajadzīgā detalizācijas pakāpe. Kā atsevišķus sabiedrības interesēs izmantojamu privātā sektora datu piemērus var minēt sociālo plašsaziņas līdzekļu datus, darījumu datus vai mazumtirgotāju datus. Arī uzņēmumi var apsvērt, kā to dati var veicināt sabiedrības interešu mērķa sasniegšanu, un sākt sarunu procesu;

b) pusēm jānosaka iekšējās problēmas un ar datu apmaiņu saistītie ierobežojumi:

   - valsts struktūrām un uzņēmumiem, iespējams, jāveic ieguldījumi zināšanu un datu pārvaldībā;
   - uzņēmumi, kas izveido korporatīvas nodaļas, kuras ir atbildīgas par datu apmaiņu, tostarp datu monetizāciju *B2B* kontekstos, konstatēs, ka datu pārvaldības, infrastruktūras un juridiskās izstrādes ziņā *B2G* datu apmaiņa ir lētāka un mazāk problemātiska. Tā kā datu apmaiņa kļūst svarīga aizvien vairāk uzņēmumiem, individuālās sadarbības izmaksas un tai uzliktais slogs varētu samazināties;
   - uzņēmumiem un valsts sektora struktūrām jānodrošina atbilstība VDAR un e-privātuma tiesību aktu noteikumiem (lai nodrošinātu apstrādes likumību, tostarp juridiskā pamata ievērošanu, piemēram, attiecībā uz piekrišanu, anonimizācijas metožu pareizu izmantošanu, konfidencialitātes ievērošanu attiecībā uz "integrētas datu aizsardzības" un "datu aizsardzības pēc noklusējuma" principu, privātumu saglabājošo analītisko metožu izmantošanu un, vajadzības gadījumā, datu aizsardzības ietekmes novērtējumiem);

26 Ja valsts iestādes balstās uz VDAR 6. panta 1. punkta e) apakšpunktu ("apstrāde ir vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs"), šāds juridiskais pamats jānosaka Savienības vai dalībvalstu tiesību aktos. Turklāt šādas "pilsonisko datu apmaiņas" gadījumā datu subjekti ir skaidri jāinformē, tostarp par tiesībām atsaukt piekrišanu un par jebkuru iespējamo viņu personas datu papildu apstrādi, ko veic valsts iestādes.

– lai nodrošinātu analīzes rezultātu reprezentativitāti, izvairoties no atlases neobjektivitātes, valsts sektora struktūrām jāveic rūpīga iespējamo datu avotu analīze un jānoskaidro viena konkrēta datu sniedzēja ierobežojumi. Tām rūpīgi jāapsver datu triangulācija, pastāvīga novērošana un modeļu atkārtota pielāgošana, kā arī kombinācija ar, piemēram, sabiedrisko apspriešanu un rīkiem, ar ko vāc pierādījumus un ieinteresēto personu viedokļus, lai mazinātu riskus un iespējamus privātā sektora datu avotu metodoloģiskos ierobežojumus;

c) attiecībā uz datu apmaiņu pusēm ir jāizvēlas tehniskie vai praktiskie nosacījumi, kas ir vislabāk piemēroti to iekšējo problēmu un datu pārvaldībai:
   – valsts struktūrām jāgarantē leģitīmo komerciālo interešu (piemēram, uzņēmumu konfidenciālās informācijas, tirdzniecības noslēpumu) aizsardzība un jāpanāk tehnisko nosacījumu drošība attiecībā uz piekļuvi privātā sektora datiem. Privātā sektora dati, ko pārsūta valsts sektora struktūrai, jāuzskata par konfidenciāliem datiem. Attiecīgajās datu apstrādes infrastruktūrās, izmantojot anotāciju un piekļuves ierobežojumus, skaidri jānorāda, ka tām piemēro noteiktus atbrīvojumus, ja uz valsts sektora struktūru attiecas tiesību akti par piekļuvi dokumentiem. Jāveic atbilstīgi pasākumi, lai panāktu tīklu un informācijas sistēmu drošību;
   – valsts struktūrām, iespējams, jāpaplašina savas tehniskās un personāla spējas izpētīt privātā sektora datu izmantošanas iespējas;

d) līgumā jāiekļauj īstenošanas nosacījumi, laika ierobežojumi un īpašas datu kopas, ko varētu izmantot:
   – valsts struktūrām jānodrošina, ka to konkrētu privāto datu pieprasījums atbilst proporcionalitātes principam un ir vajadzīgs definētā sabiedrības interešu mērķa sasniegšanai. Līgumā jānorāda, ka pēc tam, kad mērķis vai termiņa ierobežojums ir sasniegts, pārsūtītie dati ir jāizdzēš. Lai izmantotu tos pašus datus atšķirīgam mērķim, ir jāslēdz jauns vai jāgroza sadarbības līgums;
   – pusēm jādefinē nosacījumi darbības līmenī attiecībā uz datu pārsūtīšanu, proti, datu un metadatu formāts, kvalitāte, detalizācija un piekļuves ilgums un veids;
   – pusēm jānosaka kompensācija. Šajā ziņā pastāv dažādas iespējas, proti, atlīdzību paredz tikai par to izmaksu proporcionālu atgūšanu, kas radušās datu sagatavošanā, uzglabāšanā un izplatīšanā — tikai izņēmuma gadījumos tas tiek apvienots ar atļauju gūt taisnīgus ienākumus no ieguldījumiem —, un atlīdzību maksimāli paredz tikai par tām izmaksām, kas saistītas ar datu izplatīšanu, ņemot vērā to, ka datu sagatavošanas un uzglabāšanas izmaksas atkarībā no konkrētā gadījuma var jau būt segtas no citām ieņēmumu plūsmām. Iespējas izvēle varētu būt saistīta ar sasniedzamo sabiedrības interešu mērķi un apmierināmo sociālo vajadzību specifiku;
   – lai ļautu valsts struktūrām veikt vajadzīgo kvalitātes novērtēšanu un pārliecināties par to, vai ir iespējama atlases neobjektivitāte vai citi kvalitātes ierobežojumi, kas var noskaidroties tikai pēc līguma noslēgšanas,

uzņēmumiem, kuri piegādā datus, savu iespēju robežās ir jāpiedāvā saprātīgs un samērīgs atbalsts, lai dotu iespēju novērtēt norādītājiem mērķiem nepieciešamo datu kvalitāti, tostarp attiecīgā gadījumā ar iespēju veikt revīziju vai citādi pārbaudīt datus;

e) pusēm jāvienojas par kopīgiem līguma izpildes uzraudzības pamatprincipiem:
   - tās var vienoties par rīcības kodeksu vai izmantot spēkā esošos ētikas noteikumus, piemēram, Eiropas Statistikas prakses kodeksu27, izveidot koordinācijas komiteju vai iecelt neatkarīgu revidentu, kas pārrauga datu izmantošanu;
   - valsts struktūras ievieš nepieciešamos aizsardzības pasākumus, kas liedz ļaunprātīgi izmantot datus, kuriem piekļūts, citos nolūkos, nevis tajos, kas noteikti līgumā;

f) līgumā jāietver atbildības noteikumi par kļūdainu datu piegādi, pārtraukumiem datu pārraidē, nekvalitatīvu skaidrojošo darbu, ja tas tiek izplatīts kopā ar datu kopām, vai datu iznīcināšanu/nozaudēšanu vai izmainīšanu (ja tā ir nelikumīga vai nejauša), kas var radīt zaudējumus;

g) līgumā jānosaka piemērojamie tiesību akti un strīdu izšķiršanas mehānismi. Jebkurai pusei jābūt iespējai brīvi izbeigt līgumu, ja pastāv juridisks vai tehnisks risks attiecībā uz sniegto datu apstrādi vai izmantošanu;

h) valsts struktūrām jāizplata *B2G* sadarbības rezultāti/analīze un, kad tas ir nepieciešams vai lietderīgi, jānodrošina mehānismi sabiedrības viedokļa apzināšanai, neapdraudot privātā sektora datu konfidencialitāti.

27 Attiecībā uz līgumiem ar statistikas birojiem tas varētu būt Eiropas Statistikas prakses kodekss, http://ec.europa.eu/eurostat/web/products-manuals-and-guidelines/-/KS-32-11-955.

### 4.3. Tehniskie līdzekļi *B2G* sadarbības attīstīšanai

Jebkurā *B2G* sadarbībā ir jāpieņem lēmums par to, kā sabiedrības interešu labā ir iegūstami privātā sektora datu analīzes rezultāti. Tas var nozīmēt privātā sektora datu faktisku pārsūtīšanu uz attiecīgās valsts struktūras IT vidi. Tomēr tā nav vienīgā iespēja un var tikt izskatīti citi mehānismi. Šajā iedaļā sniegts pārskats par tehniskiem līdzekļiem, kas ir alternatīva privātā sektora datu pārsūtīšanai uz valsts struktūras IT vidi. Šie tehniskie mehānismi var nodrošināt piekļuves un datu izmantošanas noteikumus, vienlaikus piedāvājot uzticamu un drošu vidi datu kopu apmaiņai.

a) **Datu platformas**. Datu platformu izveide var garantēt drošu vidi datu uzglabāšanai un apmaiņai starp uzņēmumiem un valsts struktūrām. Šādas platformas var nodrošināt valsts struktūras ar standartizētiem datiem, lai sadarbībā ar uzņēmumiem izveidotu sniegto datu resursus vai sagatavotu analīzes rezultātus.

**Lielo datu statistikas centrs**, Nīderlande28

Lielo datu statistikas centrs (*CBS*) sadarbojas ar daudzām privātā sektora organizācijām, lai vāktu vajadzīgos privātā sektora datus un veidotu kvalitatīvas datu vizualizācijas. Tā kā *CBS* ir valsts sektora organizācija, tam ir piekļuve arī plašam Nīderlandes repozitorijam ar valdības un sensoru datiem, kurus tas ir spējīgs apvienot ar šiem jaunajiem datu avotiem, lai nodrošinātu jaunus analīzes rezultātus.

b) **Algoritms datiem**. Algoritma piemērošana datiem var būt risinājums datu drošības, aizsardzības un privātuma problēmu jomā. Tas ievērotu vienu no galvenajiem apsvērumiem attiecībā uz personas datu un privātuma aizsardzības nodrošināšanu, proti, pārvietot datus pēc iespējas mazāk. Šā risinājuma izmantošana nozīmē to, ka algoritms ir iekļauts privātā uzņēmuma IT vidē, kur tiek veikta analīze. Valsts sektora struktūrai atpakaļ tiek nosūtīti tikai anonīmi analīzes rezultāti, kas iegūti ar šā algoritma palīdzību. Uzņēmums un/vai attiecīgā valsts organizācija (vai uzticams starpnieks) varētu kopīgi izstrādāt datu vaicājumu saskarni un analīzes iespējas.

**Atvērtie algoritmi (*OPAL*)**29

Šis projekts ir sociāltehnoloģiska inovācija, ko izstrādājuši *Data-Pop Alliance*, Londonas Impērijas koledža, *MIT Media Lab, Orange* un Pasaules Ekonomikas forums, lai izmantotu privātā sektora datus sabiedriskā labuma mērķiem, "nosūtot kodu datiem" tādā veidā, kas saglabā privātumu, ir paredzams, iekļaujošs, mērogojams un ilgtspējīgs. Algoritma izstrādē ieguldījumu devušas vietējās padomdevējas komitejas attīstības un ētikas orientācijas jomā (*Committees for the Orientation of Development and Ethics — CODE*), lai šie algoritmi atbilstu vietējām vajadzībām un ievērotu vietējos standartus, nevis uzspiestu ārējus viedokļus un pieredzi.

28 https://www.cbs.nl/en-gb/our-services/innovation/big-data.
29 http://www.opalproject.org/about-us/

c) **Privātumu saglabājoša skaitļošana.** Pēdējos gados tika izstrādāti vairāki skaitļošanas modeļi, kas ļāva veikt operācijas ar datiem, kuriem jāpaliek konfidenciāliem. Šādi modeļi ļauj iegūt vēlamo izvadinformāciju, neatklājot ievaddatus. Tāpēc datu skaitļošana var notikt kopīgi dažādos administratīvos domēnos (publiskos vai privātos), nepārvietojot datus ārpus uzņēmuma. Šādi modeļi ietver būtisku paradigmas maiņu no "datu apmaiņas" uz "kopīgu skaitļošanu". Pašreizējo privātumu saglabājošas skaitļošanas metožu vidū drošas daudzpusējas skaitļošanas kategorija šķiet īpaši piemērota saistībā ar *B2G* sadarbību datu jomā. Dažas vienkāršas, drošas un daudzpusējas skaitļošanas metodes ir īpaši mērogojamas un iedarbīgas. Vairāki uzņēmumi jau nodrošina šo tehnoloģiju un attiecīgās platformas. Ir veikti pētījumi, kuros šī metode tika izmantota *B2G* sadarbības jomā.

**Droša daudzpusēja skaitļošana30**

Droša daudzpusēja skaitļošana ir praktiska kriptogrāfiska metode konfidenciālu datu apstrādei. Pētniecības sasniegumi ir sekmējuši tās izmantošanu privātumu saglabājošā statistikas analīzē. Igaunijas Lietišķās pētniecības centra (*CentAR*) statistiķi 2015. gadā veica lielo datu pētījumu, lai atrastu sakarības starp strādāšanu augstskolas studiju laikā un nespēju laikus pabeigt studijas. Pētījums tika veikts, sasaistot Igaunijas Nodokļu un muitas pārvaldes individuālo nodokļu maksājumu datubāzi un Izglītības un pētniecības ministrijas augstākās izglītības norišu datubāzi. Datu vākšana, sagatavošana un analīze tika veiktas, izmantojot drošu daudzpusēju skaitļošanas sistēmu *Sharemind*, kas analīzei nodrošināja pilnīgu kriptogrāfisku aizsardzību. Izmantojot analīzē desmit miljonus nodokļu uzskaites datu un pusmiljonu izglītības statistikas datu, tas ir lielākais kriptogrāfiski privātais statistikas pētījums, kas jebkad ir veikts ar reāliem datiem.

30 *Bogdanov* (un citi), "*Students and Taxes: a Privacy-Preserving Social Study Using Secure Computation*". *In Proceedings on Privacy Enhancing Technologies, PoPETs*, 2016 (3), 117.–135. lpp, 2016. gads (paplašināta versija, PDF).