Latvijas neformālais dokuments par vienkāršošanu Digitālā omnibusu paketē

Latvija atzinīgi vērtē Eiropas Komisijas iniciatīvu vienkāršot un saskaņot ES digitālo regulējumu, izmantojot gaidāmo Digitālo omnibusu. Tās mērķim jābūt uzlabot saskaņotību un samazināt lieku administratīvo slogu, vienlaikus saglabājot politiskos mērķus un esošo tiesību aktu aizsardzības līmeni.

Vienkāršošanai jābūt vērstai uz praktisku īstenošanu, juridisko skaidrību un konsekventu interpretāciju visās dalībvalstīs, izvairoties no iespējamiem pretrunīgiem skaidrojumiem un pārklājošām procedūrām starp dažādām iesaistītajām iestādēm. Uzsvars jāliek uz to, kā noteikumi darbojas praksē, nevis uz jau panākto politisko kompromisu pārskatīšanu.

1. **Pārvaldība un koordinācija**

Digitālā regulējuma īstenošana ir radījusi arvien lielāku padomju, iestāžu un koordinācijas formātu skaitu. Lai mazinātu sadrumstalotību, Latvija piedāvā:

- Izveidot un uzturēt kopīgu digitālo terminu glosāriju, ko izmantot visā acquis.
- Efektīvāk izmantot esošās Eiropas koordinācijas struktūras (AI padome, Eiropas datu inovāciju padome, Interoperable Europe padome, ENISA), lai nodrošinātu konsekventu piemērošanu.
- Ļaut dalībvalstīm elastīgi konsolidēt nacionālās kompetences un izvairīties no paralēlām iestādēm. Nodrošināt saprātīgu īstenošanas termiņu.
- Organizēt regulāras tehniskās apmaiņas starp dalībvalstīm pirms būtiskiem īstenošanas termiņiem, lai savlaicīgi identificētu kopīgus izaicinājumus.
- Nodrošināt pastāvīgu koordināciju un proaktīvas, savlaicīgas vadlīnijas starp dalībvalstu iestādēm un Eiropas Komisiju, citām ES institūcijām, struktūrām un kompetenču centriem (AI birojs, Eiropas datu inovāciju padome (EDIB), ENISA u.c.), lai nodrošinātu konsekventu piemērošanu un interpretāciju.
- Ieviest vienotu "Digitālās atbilstības sistēmu" ES līmenī, kas ļautu uzņēmumiem izmantot vienotu atbilstības un ziņošanas mehānismu, lai izpildītu vairāku regulu prasības, harmonizēt incidentu ziņošanas un risku novērtēšanas formātus, savstarpēji atzīt drošības un atbilstības pasākumus dažādos regulējumos (piemēram, DORA un GDPR).

2. **Mākslīgā intelekta akts**

Latvija atbalsta samērīgu, inovācijām draudzīgu AI akta īstenošanu un Digitālā omnibusa mērķi vienkāršot un harmonizēt ES digitālo regulējumu, īpaši tur, kur īstenošana rada lieku administratīvo slogu. Digitālajam omnibusam vajadzētu:

- Precizēt, kas tiek uzskatīts par augsta riska MI, sniedzot interpretatīvas vadlīnijas par augsta riska MI un tradicionālo (ne-MI) algoritmu apstrādi. Nepieciešamas kodolīgas, praksē orientētas vadlīnijas, piemēri, kontrolsaraksti un veidlapas klasifikācijai, incidentu ziņošanai un saistītajiem procesiem.
- Nodrošināt ES veidlapu paraugus, lai standartizētu atbilstības dokumentāciju un pēcpārdošanas uzraudzību, samazinot mainīgumu un sarežģītību dalībvalstu starpā.

- Atbalstīt MVU un zema riska publiskā sektora izmantošanu, paplašinot un precizējot MVU specifiskās elastības, tostarp publiskām iestādēm, kas izmanto zema riska sistēmas, lai atbilstība būtu samērīga un neveicinātu atbildīgu inovāciju.
- Atzīt regulatīvās smilškastes, pieņemot to rezultātus kā derīgu atbilstības pierādījumu, atbalstot agrīnu sadarbību ar regulatoriem un drošu eksperimentēšanu.
- Izvairīties no paralēlām tehniskajām dokumentācijām un deklarācijām, tiecoties uz vienu modulāru tehnisko dokumentu un vienu ES atbilstības deklarāciju katrai sistēmai, atkārtoti izmantojot kopīgus pierādījumus visos piemērojamos aktos, pilnībā saglabājot prasības par drošību, robustumu un kiberdrošību. Piemēram, vienots "MI + kiberdrošība" tehniskais dokuments varētu būt pamats vienai deklarācijai, izvairoties no sadrumstalotām procedūrām, vienlaikus saglabājot augstu uzticības līmeni.
- Padarīt MI pratību praktiski īstenojamu, ieviešot bezmaksas tiešsaistes apmācības un kodolīgas vadlīnijas ar kontrolsarakstiem, veidlapām un piemēru darba plūsmām – lai organizācijas varētu praktiski un ar zemu birokrātiju attīstīt darbinieku kompetences.
- Nodrošināt juridisko noteiktību, kad standarti atpaliek, sniedzot skaidrus aizstājējmehānismus un drošu patvērumu dokumentētiem, labticīgiem operatoriem, īpaši MVU. Atbilstības termiņiem jābūt reāliem, un uzraudzībai – samērīgai, ņemot vērā patiesus centienus ievērot pieejamās vadlīnijas un alternatīvus ceļus atbilstības demonstrēšanai.
- Saskaņot MI aktu un GDPR, nodrošinot skaidru, vienotu abu aktu interpretāciju (īpaši par riska klasifikāciju un datu izmantošanu) un ieviest vienotu, racionalizētu atbilstības procesu: viena procedūra, viens ietekmes novērtējums, viens dokumentu komplekts, aptverot gan pamattiesību, gan datu aizsardzības riskus. Tam jābūt atbalstītam ar praktisku ES līmeņa rīku un vienkāršiem kontrolsarakstiem, lai organizācijas, īpaši publiskās iestādes, jaunuzņēmumi un MVU, varētu efektīvi nodrošināt atbilstību. Paātrināt e-privātuma noteikumu pārskatīšanu, lai tie atspoguļotu pašreizējo tehnoloģisko realitāti un nodrošinātu saskaņotību ar MI aktu un GDPR, mazinot juridisko sadrumstalotību MI darbinātajiem pakalpojumiem.

3. Datu regulējums

Atbalstām mērķi harmonizēt un vienkāršot esošos datu noteikumus, lai izveidotu skaidru, saprotamu un efektīvu tiesisko regulējumu, kas veicina drošu un efektīvu datu apmaiņu starp uzņēmumiem un publiskā sektora iestādēm. Datu aizsardzība un privātums ir neatņemama pamattiesību sastāvdaļa, un to ievērošana jānodrošina visā vienkāršošanas procesā. Tāpēc ir būtiski saglabāt līdzsvaru starp caurskatāmību, datu pieejamību un personas datu aizsardzību, nodrošinot, ka regulējums ir ne tikai efektīvs un praktiski īstenojams, bet arī pilnībā saderīgs ar cilvēktiesībām.

Pašreizējais datu regulējums – Datu akts, Datu pārvaldības akts (DGA), Regula par nepersonas datu brīvu apriti (FFDR) un Atvērto datu direktīva – gūtu labumu no skaidrākas mijiedarbības un vienkāršākas pārvaldības. Daži risināmie jautājumi:

- DGA nosaukums ir diezgan maldinošs, jo tas patiesībā neaptver datu pārvaldības tēmu. Regulu pārskatīšanas procesā piedāvājam šo aspektu integrēt grozītās regulas tvērumā.
- Pārvaldības struktūra – ir daudz kontaktpunktu un kompetento iestāžu. Vienkāršošanas procesā šis jautājums jārisina, ņemot vērā, kā visas šīs institūcijas mijiedarbosies ar EDIB.
- Ar Datu aktu EDIB mandāts ir paplašinājies, aptverot ne tikai valdības datus, bet arī privātā sektora datu darījumus. Abas svarīgās atbildības jāatspoguļo EDIB darba kārtībā.
- Regulējuma vienkāršošanas ziņā atbalstām PSI direktīvas integrāciju DGA, kā arī FFDR kopā ar privātā sektora orientētajiem DGA elementiem (datu altruismu organizāciju un datu starpnieku pakalpojumu reģistrācija) integrāciju Datu aktā. Tomēr uzskatām, ka datu pārvaldības aspekti jāintegrē, lai datu regulējums būtu vieglāk saprotams.
- Attiecībā uz INSPIRE direktīvu un gaidāmo iniciatīvu "GreenData4All" uzskatām, ka tai jābalstās uz konkrētiem lietošanas gadījumiem, lai nodrošinātu skaidru mērķi un caurspīdīgas saiknes ar citiem datu regulējumiem. No praktiskā viedokļa iesakām pārskatīt pašreizējās datu formātu prasības, lai padarītu INSPIRE datus lietojamākus dažādās nozarēs. Pašlaik noteiktie formāti ir ļoti specifiski un, cik zināms, plaši netiek izmantoti ārpus ģeotelpiskās jomas, ierobežojot plašāku atkārtotu izmantošanu.

4. Administratīvais slogs valsts pārvaldēm

Dažādu digitālo aktu kopējais efekts ir radījis sarežģītas ziņošanas un koordinācijas prasības dalībvalstīm. Lai nodrošinātu īstenošanas ilgtspēju, jārisina šādi jautājumi:

Kartēt un racionalizēt visas ziņošanas saistības, kas izriet no digitālā acquis.

Ieviest kopīgas digitāli iespējotas veidlapas un ziņošanas ciklus, lai samazinātu dublēšanos.

Pielietot principu "viens iekšā, viens ārā" arī attiecībā uz prasībām, kas tiek uzliktas nacionālajām administrācijām.

Izveidot vienotu atsauces portālu definīcijām, veidlapām un vadlīnijām, kas tiek izmantotas digitālajā regulējumā.

Nodrošināt kopīgas vadlīnijas un apmācību materiālus amatpersonām, kas iesaistītas MI akta, Datu akta un saistīto instrumentu piemērošanā.

Izveidot vienkāršu kanālu nepārtrauktai atgriezeniskajai saitei no dalībvalstīm Eiropas Komisijai par īstenošanas jautājumiem.

Elektroniskā identitāte

Ir būtiski nodrošināt regulatīvo un operatīvo saskaņotību ar gaidāmo ES Digitālās identitātes maku un ES Uzņēmumu maku.

Līdz 2026. gada 24. decembrim katrai dalībvalstij jānodrošina, ka tās iedzīvotājiem ir pieejams vismaz viens Eiropas Digitālās identitātes maks. Ņemot vērā, ka Eiropas Uzņēmumu maka funkcionālais un juridiskais regulējums vēl nav definēts, Digitālā omnibusa paketei būtu jāizvērtē iespēja izstrādāt Eiropas Uzņēmumu maku Eiropas Digitālās identitātes maka ietvaros.

5. Kiberdrošība

Kiberdrošības jomā aicinām harmonizēt incidentu ziņošanu. Pašlaik incidentu ziņošanas prasības pārklājas GDPR, NIS2, DORA un CER regulējumos. Incidenti bieži šķērso regulatīvās robežas, piemēram, daudzi personas datu incidenti ir arī kiberdrošības incidenti. Uzņēmumi šādās situācijās labprātāk iesniegtu vienu konsolidētu ziņojumu, nevis atsevišķus katrai uzraudzības iestādei.

Eiropas Komisija ir atzinusi nepieciešamību pēc pasākumiem, kas mazinātu incidentu ziņošanas sarežģītību, vienkāršotu atbilstības prasības un veicinātu kiberdrošības incidentu ziņošanas rīku izmantošanu, vienlaikus saglabājot augstu kiberdrošības līmeni. Izvērtējot iespējamo vienotas ziņošanas platformas izveidi, lai atvieglotu kiberdrošības incidentu ziņošanas prasības, ir svarīgi, lai šāda platforma būtu viegli administrējama un lietotājam draudzīga visiem tās lietotājiem – uzņēmumiem (piemēram, NIS2 subjektiem), uzraudzības iestādēm un ES institūcijām – un būtu savietojama.

Aicinām arī izstrādāt mehānismu, kas harmonizētu kiberdrošības regulējumus starp ES dalībvalstīm. Pašlaik valstis interpretē regulējumus dažādi un piemēro tos dažāda lieluma, apgrozījuma, nozaru un kritiskuma līmeņa subjektiem. Atšķirīgo nacionālo tiesību aktu dēļ ES mēroga kiberdrošības regulējumi bieži tiek piemēroti nevienmērīgi noteiktās nozarēs. Tas rada risku traucēt godīgu konkurenci starp dažādu valstu uzņēmumiem. Lai neietekmētu brīvo tirgu visās ES valstīs, nepieciešama vienota kiberdrošības regulējumu piemērošana. Uzskatām, ka to var panākt, uzlabojot koordināciju, informācijas apmaiņu un pieredzes apmaiņu starp dalībvalstīm.

6. GDPR un e-Privātuma direktīva

Noteikumi par sīkdatnēm ir jāvienkāršo, jo tie attiecas gan uz GDPR, gan e-Privātuma direktīvu. Prasība pēc piekrišanas būtu jāpadara vienkāršāka, piemēram, ja runa ir par zema riska sīkdatnēm, kas tiek izmantotas analītikai vai statistikai.

GDPR un datu apmaiņas kontekstā nepieciešama lielāka skaidrība. Pašlaik nosacījumi datu nodošanai trešajām valstīm ir diezgan apgrūtinoši, lai gan realitātē datu plūsma notiek nepārtraukti. Jāizstrādā mehānismi, kas atvieglotu šādu apmaiņu un padarītu atbilstības uzraudzību vienkāršāku.