IKT risinājumi, prasības un procedūras drošai aizsargājamo datu izmantošanai pētniecībā

Augstākās izglītības un zinātnes informācijas tehnoloģijas koplietošanas pakalpojumu centrs

Versija 1.2

2026. gada 15. maijā

Saturs

Izmantotie saīsinājumi un termini

Tabula 1 - Izmantotie saīsinājumi un termini

Saīsinājums / Termins	Skaidrojums
Anonimizācija	Anonimizācija ir process, kurā dati tiek pilnībā pārveidoti tā, lai vairs nebūtu iespējams identificēt konkrētu personu, pat izmantojot papildu informāciju. Lai to panāktu, var tikt izmantotas speciālas metodes un rīki, kas nodrošina datu neatgriezenisku pārveidošanu.
API	Lietojumprogrammu saskarne (angļu val. Application Programming Interface)
AWS	Amazon mākoņdatošanas platforma un pakalpojumu kopums (angļu val. Amazon Web Services)
Azure	Microsoft mākoņdatošanas platforma
B2Drop	Pētniecības datiem paredzēts mākoņglabāšanas un failu koplietošanas pakalpojums
CSP	Centrālā statistikas pārvalde
Datu rezidence	Prasība vai prakse, ka dati tiek glabāti un apstrādāti noteiktā valstī vai reģionā atbilstoši juridiskajiem, līgumiskajiem vai organizācijas noteiktajiem nosacījumiem.
DPA	Datu pārvaldības akts (angļu val. Data Governance Act)
EHDS	Eiropas veselības datu telpas regula (angļu val. European Health Data Space Regulation)
EOSC	Eiropas atvērtās zinātnes mākonis (angļu val. European Open Science Cloud) - federēta Eiropas pētniecības datu un pakalpojumu ekosistēma zinātnes vajadzībām
ES	Eiropas Savienība
EVDT	Eiropas veselības datu telpa (angļu val. European Health Data Space).
FAIR	FAIR principi ir datu pārvaldības un kopīgošanas principi, kas paredz, ka dati ir atrodami, pieejami, sadarbspējīgi un atkārtoti izmantojami (angļu val. Findable, Accessible, Interoperable, Reusable).
FileSender	Droša lielapjoma failu nosūtīšanas un koplietošanas platforma
GCP	Google mākoņdatošanas platforma (angļu val. Google Cloud Platform)
Gmail	Google e-pasta pakalpojums
Google Drive	Google mākoņglabāšanas un failu koplietošanas pakalpojums
GPU	Grafiskais procesors (angļu val. Graphics Processing Unit)
HIPAA	Veselības apdrošināšanas pārnesamības un atbildības likums (angļu val. Health Insurance Portability & Accountability Act)
HPC	Augstas veiktspējas skaitļošana (angļu val. High Performance Computing)
IKT	Informācijas un komunikācijas tehnoloģijas
IT	Informācijas tehnoloģijas
MI	Mākslīgais intelekts
MFA	Multi faktoru autentifikācija (angļu val. Multi factor authentication)
MFT	Pārvaldīta failu pārsūtīšana (angļu val. Managed File Transfer)
NextCloud	Atvērtā koda failu glabāšanas, sinhronizācijas un koplietošanas platforma
OneDrive	Microsoft mākoņglabāšanas un failu sinhronizācijas pakalpojums
Outlook	Microsoft e-pasta pakalpojums
ownCloud	Atvērtā koda failu glabāšanas, sinhronizācijas un koplietošanas platforma

Saīsinājums / Termins	Skaidrojums
Pseidonimizācija	Pseidonimizācija ir process, kurā personas dati tiek aizvietoti ar izdomātiem identifikatoriem (pseidonīmiem), piemēram, ar unikāliem kodiem vai numuriem, saglabājot iespēju atjaunot sākotnējo informāciju, ja tas nepieciešams pētījuma mērķu sasniegšanai. Šo procesu var veikt gan manuāli, gan ar IT rīku palīdzību.
Python	Augsta līmeņa programmēšanas valoda, ko plaši izmanto datu analīzē, mākslīgajā intelektā un programmatūras izstrādē
R	Atvērtā koda programmēšanas valoda un vide statistiskajai skaitļošanai, datu apstrādei un vizualizācijai
RTU	Rīgas Tehniskā universitāte
SATRE	Uzticamas pētniecības vides standartarhitektūra (angļu val. Standard Architecture for Trusted Research Environments) - ietvars šādas vides projektēšanai, novērtēšanai un pārvaldībai
SFTP	Drošs failu pārsūtīšanas protokols, kas balstīts uz SSH (angļu val. SSH File Transfer Protocol / Secure File Transfer Protocol)
Sharepoint	Microsoft mākoņglabāšanas un failu sinhronizācijas pakalpojums
SPE	Drošas apstrādes vide (angļu val. Secure processing environment)
SPSS	IBM produkts - statistikas datu analīzes programmatūra (angļu val. Statistical Package for the Social Sciences)
SSH	Kriptogrāfisks tīkla protokols (angļu val. Secure Shell) drošai attālinātai piekļuvei sistēmām un komandu izpildei
Teams	Microsoft sadarbības un saziņas platforma tērzēšanai, sapulcēm, zvaniem un failu koplietošanai
TLS	Transporta slāņa drošības protokols (angļu val. Transport Layer Security), kas nodrošina šifrētu datu pārraidi tīklā.
VDAR	Vispārējā datu aizsardzības regula
VPN	Virtuālais privātais tīkls (angļu val. Virtual Private Network)
WebDAV	HTTP protokola paplašinājums attālinātai failu pārvaldībai un koplietošanai (angļu val. Web Distributed Authoring and Versioning)

Ievads

Mūsdienu pētniecībā arvien lielāka nozīme ir piekļuvei trešo pušu datiem, kas atrodas ārpus pašu pētnieku vai zinātnisko institūciju rīcības, tostarp personas datiem, īpašu kategoriju datiem, komerciāli sensitīvai informācijai, intelektuālā īpašuma elementiem un citiem publiski nepieejamiem datiem. Vienlaikus viens no būtiskākajiem šķēršļiem šādu datu izmantošanai pētniecībā ir datu avotu bažas par datu drošību, neatbilstošu izmantošanu un nepietiekami kontrolētu piekļuvi nodošanas gadījumā.

Lai šādu datu izmantošana pētniecībā būtu droša, pārskatāma un praktiski īstenojama, ir nepieciešama ne tikai atbilstoša datu pārvaldība, bet arī pārdomāta IKT risinājumu un procesa organizācijas pieeja. Tas ietver lēmumus par to, kādā vidē dati tiek saņemti, glabāti, kopīgoti, apstrādāti un publicēti, kā tiek organizēta piekļuve datiem, kādas drošības prasības jāievēro un kā tiek pārvaldīti ar datu izmantošanu saistītie riski visā pētniecības dzīves ciklā.

Dokumenta mērķis

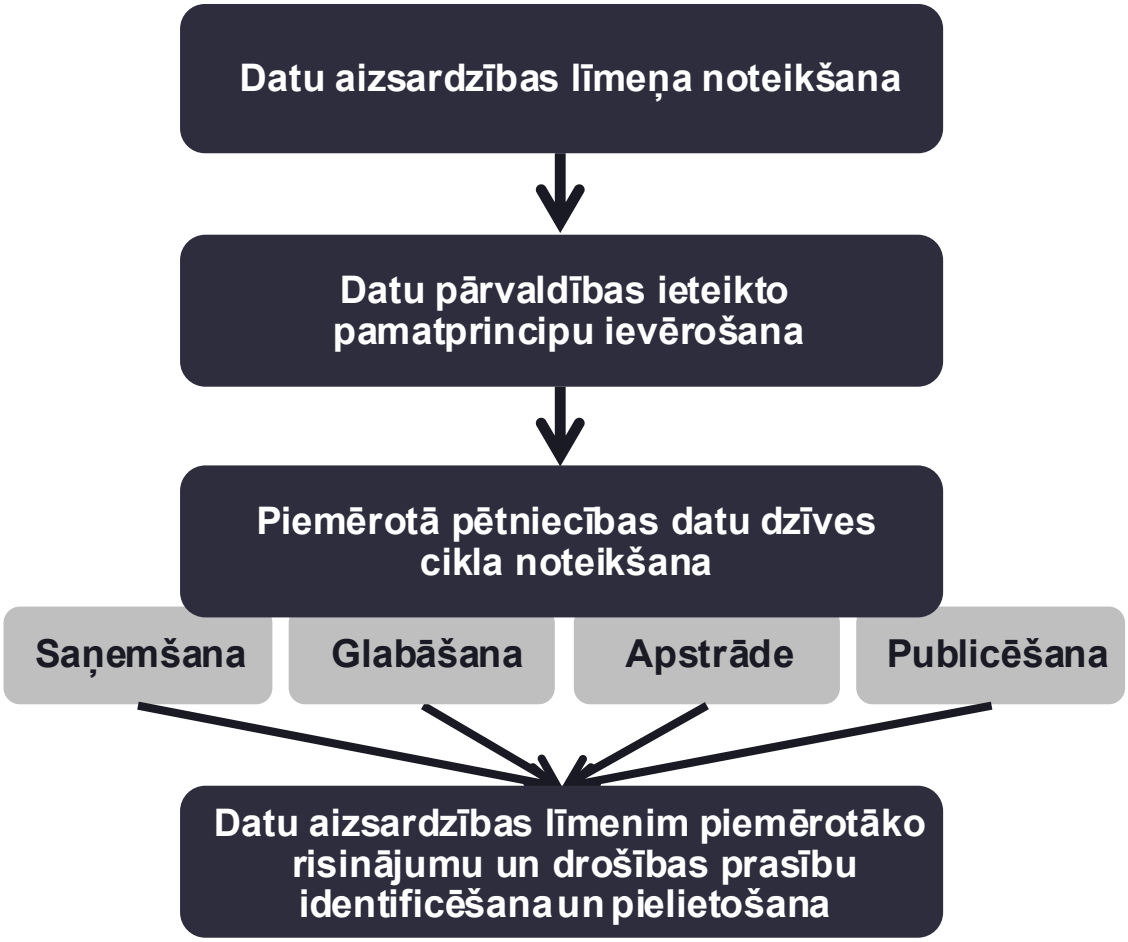
Dokumenta mērķis ir noteikt praktiski piemērojamu ietvaru IKT risinājumiem, prasībām un procedūrām, kuras zinātniskajām institūcijām un pētniekiem ieteicams ievērot, izmantojot aizsargājamus datus pētniecībā, tādējādi nodrošinot nepieciešamo datu drošības līmeni, aizsargātu datu avotu intereses un vienlaikus saglabātu iespēju praktiski ieviest to pētniecības vidē.

Šo rekomendāciju sagatavošanai tika veikta analīze par pašreizējo pētniecības datu pārvaldības praksi, kuras ietvaros tika apzināti augstākās izglītības un zinātnisko institūciju, kā arī potenciālo datu sniedzēju no valsts un privātā sektora skatījumi un pieredze. Analīzes rezultāti apkopoti dokumentā “Analīze par pašreizējo pieredzi pētniecības datu pārvaldības praksē”. Rekomendāciju izstrādē tika izmantoti arī kiberdrošības un vispārējās datu pārvaldības labās prakses resursi, tostarp Nacionālais kiberdrošības likums un citi avoti, kas norādīti dokumenta sadaļā - Informācijas resursi par datu pārvaldību un ieteikto praksi.

Materiāls izstrādāts projekta “Atbalsts atvērtās zinātnes ieviešanai praksē, kā arī izveidoti risinājumi zinātnes datu koplietošanai un dalībai ES atvērtajā zinātnes mākonī” ietvaros (ANM projekta Nr. 2.1.3.1.i) ar Eiropas Savienības Atveseļošanas fonda un Latvijas valsts finansiālo atbalstu, kura ietvarā SIA “Ernst & Young Baltic” biedrības "Augstākās izglītības un zinātnes informācijas tehnoloģijas koplietošanas pakalpojumu centrs" vajadzībām analizē esošo pētniecības datu pārvaldības praksi un sagatavo rekomendācijas par IKT risinājumiem, prasībām un procedūrām drošai aizsargājamo datu izmantošanai pētniecībā.

Kā lasīt dokumentu

Šo dokumentu ieteicams izmantot kā praktisku palīglīdzekli, izvērtējot, kādas prasības un kādi risinājumi ir piemērojami konkrētā datu izmantošanas gadījumā. Dokumenta saturs ir strukturēts tā, lai lasītājs varētu soli pa solim noteikt, kāds datu aizsardzības līmenis piemērojams uz konkrētajiem datiem un kādas prasības jāievēro attiecīgajā pētniecības dzīves cikla posmā.



Attēls 1 –Skaidrojoša vizualizācija kā lasīt šo dokumentu

Informācijas resursi par datu pārvaldību un ieteikto praksi

- **Nacionālās kiberdrošības likums.** Pieejams: https://likumi.lv/ta/id/353390
- **Technical Implementation Guidance On Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures June 2025, Version 1.0** Pieejams: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf
- **Design choices for productive, secure, data-intensive research at scale in the cloud**. Pieejams: https://arxiv.org/pdf/1908.08737
- **Standard Architecture for Trusted Research Environments (SATRE).** Pieejams: https://satre-specification.readthedocs.io/en/stable/index.html
- **Data Management Expert Guide (DMEG).** Pieejams: https://dmeg.cessda.eu/
- **The Research Data Management Toolkit for Life Sciences**. Pieejams: https://rdmkit.elixir-europe.org/
- **EUDAT Collaborative Data Infrastructure**. Pieejams: https://eudat.eu/
- **Design a secure research environment for regulated data**. Pieejams: https://learn.microsoft.com/en-us/azure/architecture/ai-ml/architecture/secure-compute-for-research
- **The Five Safes**. Pieejams: https://fivesafes.org/
- **EOSC-ENTRUST: European network of trusted research environments**. Pieejams: https://eosc-entrust.eu/
- **NIST Research Data Framework (RDaF), Version 2.0 – NIST SP 1500-18r2**. Pieejams: https://www.nist.gov/publications/nist-research-data-framework-rdaf-version-20
- **Research and Engineering Studio on AWS** Pieejams: https://aws.amazon.com/hpc/res/
- **The Turing Data Safe Haven** Pieejams: https://data-safe-haven.readthedocs.io/en/latest/
- **Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products** Pieejams: https://www.cisa.gov/sites/default/files/2025-01/joint-guide-secure-by-demand-priority-considerations-for-ot-owners-and-operators-508c_0.pdf
- **Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations NIST Special Publication 800-171** Pieejams: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
- **IT-Grundschutz-Compendium** Pieejams: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.pdf?__blob=publicationFile&v=2
- **CIS Benchmarks List** Pieejams: https://www.cisecurity.org/cis-benchmarks

1. Pētniecības datu aizsardzības līmeņa klasifikācija

Pētniecībā izmantotie dati var būt ļoti atšķirīgi, sākot no publiski pieejamas informācijas līdz datiem, kuru neatbilstoša izmantošana vai izpaušana var radīt būtisku kaitējumu personām, organizācijām vai sabiedrībai kopumā. Datu klasifikācija palīdz noteikt, kāds aizsardzības līmenis katram datu veidam ir piemērojams un kādi nosacījumi jāievēro to apstrādē, glabāšanā un kopīgošanā. Datu klasifikācija ir īpaši nozīmīga personas datu apstrādes gadījumā, jo arī šajā jomā pastāv atšķirīgi sensitivitātes līmeņi, piemēram, vispārīgi personas dati un īpašu kategoriju personas dati, kuriem nepieciešami stingrāki drošības un pārvaldības pasākumi.

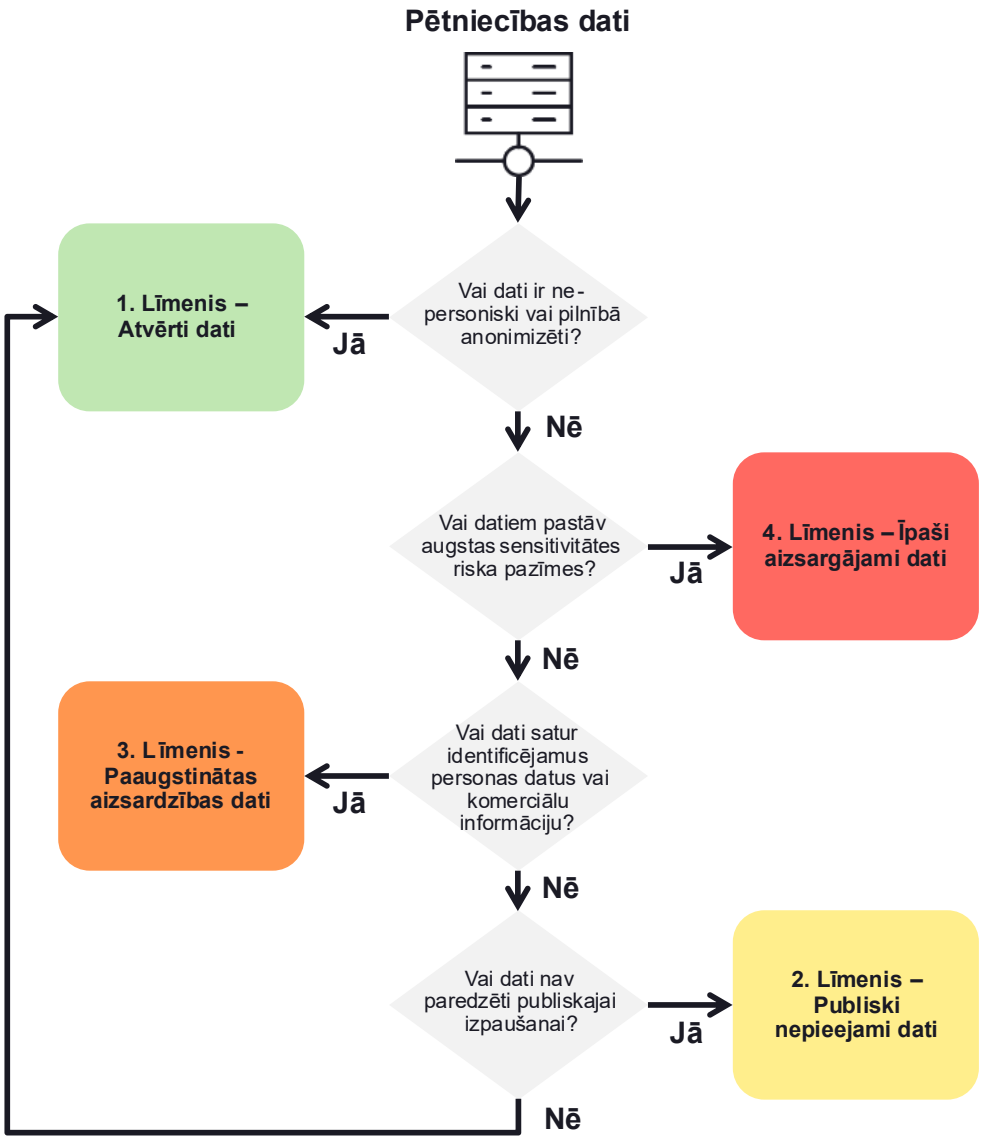
Papildus aizsardzības pasākumu noteikšanai, datu klasifikācijas līmenis var arī ierobežot, kur un kā šie dati drīkst tikt turpmāk glabāti vai apstrādāti. Atkarībā no datiem var tikt noteiktas prasības attiecībā uz datu glabāšanas vidi, piemēram, pienākums izmantot tikai konkrētas organizācijas pārvaldītas informācijas sistēmas, aizliegums datus glabāt publiskajos mākoņpakalpojumos vai ārpus noteiktas ģeogrāfiskās lokācijas.

Datu aizsardzības līmeņa noteikšanas pieeja

Datu aizsardzības līmenis nosakāms jau pētījuma plānošanas posmā, pirms dati tiek saņemti, glabāti vai nodoti apstrādei. Par sākotnējo izvērtējumu parasti atbild pētnieks vai projekta atbildīgā persona, jo tie vislabāk spēs noteikt, kādi dati tiks izmantoti, kādam mērķim tie nepieciešami, kādā apjomā un kādā veidā tos paredzēts apstrādāt. Ja datu aizsardzības līmenis nav viennozīmīgi nosakāms vai datu izmantošana var radīt paaugstinātu juridisku, tehnisku, ētisku vai drošības risku, izvērtējums veicams sadarbībā ar institūcijas atbalsta funkcijām, piemēram, datu kuratoru, datu aizsardzības speciālistu, juridisko atbalstu vai IT atbalstu.

Datu aizsardzības līmenis nav vērtējams tikai vienu reizi projekta sākumā. Tas ir jāpārskata, ja projekta gaitā būtiski mainās datu izmantošanas apstākļi, piemēram, tiek pievienoti jauni datu avoti, dati tiek sasaistīti ar citām datu kopām, projektā tiek iesaistīti jauni ārējie partneri vai mainās plānotais datu kopīgošanas, publicēšanas vai atkārtotas izmantošanas modelis. Šādos gadījumos iepriekš noteiktais aizsardzības līmenis var vairs neatbilst faktiskajam riskam, un datiem var būt nepieciešami papildu pārvaldības vai tehniskie aizsardzības pasākumi.

Datu klasifikācija nosakāma, ņemot vērā ne tikai pašu datu saturu, bet arī to izmantošanas kontekstu, kombinēšanu ar citām datu kopām, plānoto apstrādi un iespējamo ietekmi neatļautas izpaušanas vai atkārtotas identificēšanas gadījumā.



Pētniecības datu aizsardzības līmeņa klasifikācija

1. Līmenis – Atvērti dati	Ne-personiski, pilnībā anonimizēti vai apkopoti dati un ar tiem saistīti materiāli, kuru publiska pieejamība nerada būtisku risku un ir piemērota atklātai publicēšanai un brīvai atkārtotai izmantošanai.
2. Līmenis – Publiski nepieejami dati	Iekšējie pētniecības un projektu dati ar zemu jutību, kas nav paredzēti publiskai izpaušanai, bet kuru neatļauta atklāšana radītu tikai ierobežotu operatīvu vai reputācijas kaitējumu.
3. Līmenis - Paaugstinātas aizsardzības dati	Identificējami personas dati, pseidonimizēti dati, komerciāli jutīga, līgumiski ierobežota vai ar intelektuālo īpašumu saistīta informācija, kurai nepieciešama kontrolēta piekļuve un aizsardzība pret nepamatotu izpaušanu.
4. Līmenis – Īpaši aizsargājami dati	Ļoti augstas sensitivitātes dati, tostarp īpašo kategoriju personas dati un stratēģiski vai ētiski kritiska informācija, kuru neatļauta izmantošana vai atkārtota identificēšana var radīt nopietnu kaitējumu un kam nepieciešami visstingrākie aizsardzības pasākumi.

Attēls 2 – Pētniecības datu aizsargājamības līmeņa noteikšanas gaita

Tabula 2 – Datu aizsardzības līmeņa klasifikācija atbilstoši datu veidam vai kategorijai

Datu veids / kategorija pētniecībā	Vai tie iekļauj personas datus?	Piedāvātais aizsardzības līmenis	Piemēri pētījumos	Kāpēc šis līmenis tiek piedāvāts?	Gadījumi, kad aizsardzības līmenis jāpaaugstina
Publiski pieejami dati bez personas datiem un bez konfidenciāla satura	Nē	1. Atvērtie dati	Normatīvie akti; publiski pieejami ziņojumi; uzņēmumu gada pārskati; publiskas datu kopas, kurās nav personu informācijas.	Dati ir brīvi pieejami un to izpaušana nerada risku personām vai organizācijām.	Ja, apvienojot ar citiem avotiem, var noteikt personu vai atklāt aizsargājamu informāciju – jāpaaugstina vismaz uz 3. līmeni.
Pilnībā anonimizēti pētījuma dati	Nē	1. Atvērtie dati	Datu kopa, kurā neatgriezeniski noņemti visi elementi, kas ļauj noteikt konkrētu personu.	Ja anonimizācija ir pilnīga, dati vairs nav uzskatāmi par personas datiem.	Ja pastāv šaubas par anonimizācijas pilnīgumu vai datus var sasaistīt ar citiem avotiem – jāpaaugstina vismaz uz 3. līmeni.
Pētījuma darba materiāli (iekšējai lietošanai)	Parasti nē	2. Publiski nepieejami dati	Darba versijas, piezīmes, starprezultāti, iekšējie pētījuma plāni un darba dokumenti.	Nav paredzēti publiskošanai, taču parasti nerada būtisku kaitējumu, ja netiek izplatīti ārpus projekta.	Ja materiālos ir personas dati, komercinformācija vai intelektuālā īpašuma objekti – jāpaaugstina uz 3. vai 4. līmeni atkarībā no satura.
Paraugdati/sintētiski dati (testiem, mācībām), kas nav veidoti no reāliem aizsargājamiem ierakstiem	Nē	2. Publiski nepieejami dati	Piemēru datu faili, demonstrācijas komplekti, apmācību paraugi, kas nav saistīti ar reālām personām vai reāliem uzņēmuma noslēpumiem.	Šādi dati paredzēti iekšējai lietošanai un parasti nav augsta riska.	Ja paraugdati faktiski ir atvasināti no reāliem datiem vai ļauj atpazīt reālas personas/organizācijas – jāpaaugstina uz 3./4. līmeni.
Interviju ieraksti un transkripti; aptauju atbildes (ja var noteikt dalībnieku)	Jā	3. Paaugstinātas aizsardzības dati	Audio/video ieraksti; interviju transkripti; brīvteksta atbildes, kur minēti vārdi, darba vietas, amati, dzīves notikumi u. tml.	Šie dati attiecas uz personām, un neatļauta izpaušana var radīt privātuma pārkāpumu.	Ja intervijās/aptaujās parādās sensitīvie dati (piem., veselība, politiskie uzskati) vai dalībnieki ir bērni/ievainojami pieaugušie – jāpaaugstina uz 4. līmeni.
Tieši identificējami personas dati	Jā	3. Paaugstinātas aizsardzības dati	Vārds, uzvārds, personas kods, adrese, tālrunis, e-pasts, fotoattēls, balss ieraksts.	Persona ir nosakāma uzreiz; dati nav publiskojami un piekļuve tiem ir ierobežojama.	Ja dati ietver sensitīvus datus vai ja datu apjoms, detalizācijas pakāpe vai apstrādes konteksts rada paaugstinātu risku datu

Datu veids / kategorija pētniecībā	Vai tie iekļauj personas datus?	Piedāvātais aizsardzības līmenis	Piemēri pētījumos	Kāpēc šis līmenis tiek piedāvāts?	Gadījumi, kad aizsardzības līmenis jāpaaugstina
					subjektam – jāpaaugstina uz 4. līmeni.
Netieši identificējami personas dati (identificēšana iespējama kombinējot pazīmes)	Jā	3. Paaugstinātas aizsardzības dati	Vecums + amats + iestāde; reta profesija mazā kolektīvā; detalizēts notikumu apraksts, kas ļauj atpazīt personu.	Ar saprātīgiem līdzekļiem var noteikt, par kuru personu ir runa, pat ja nav vārda.	Ja dati ietver sensitīvus datus vai ja datu kombinācija, apjoms vai apstrādes konteksts rada paaugstinātu risku datu subjektam – jāpaaugstina uz 4. līmeni.
Pseidonimizēti personas dati	Jā	3. Paaugstinātas aizsardzības dati	Datu kopa ar kodiem (ID); atsevišķi glabāta "atslēga"/tabula, kas ļauj atjaunot saikni ar personu.	Pseidonimizācija samazina risku, bet saikni ar personu var atjaunot, tāpēc dati joprojām ir personas dati.	Ja pseidonimizētie dati ietver sensitīvus datus un ir viegli sasaistāmi ar citiem avotiem – jāpaaugstina uz 4. līmeni.
Uzņēmumu dati (komercdati), kas nav publiski pieejami	Atkarīgs	3. Paaugstinātas aizsardzības dati	Nepubliski finanšu rādītāji; klientu/piegādātāju saraksti; cenu politika; iekšējie darbības rādītāji; procesu apraksti.	Neatļauta izpaušana var radīt kaitējumu uzņēmuma interesēm vai līgumisku atbildību.	Ja datu avots norāda, ka dati ir komercnoslēpums, vai ja izpaušana var radīt smagas konkurences/stratēģiskas sekas – jāpaaugstina uz 4. līmeni.
Trešo pušu dati, kas nodoti pētniecībai ar līguma ierobežojumiem	Atkarīgs	3. Paaugstinātas aizsardzības dati	Datu avota (iestādes/uzņēmuma/arhīva) nodotas datu kopas, kur līgumā noteikts: kam drīkst piekļūt, kā drīkst izmantot, vai drīkst publicēt.	Līgumā noteikti ierobežojumi jāievēro, par neatļautu izpaušanu var iestāties atbildība.	Ja līgumā noteikts visaugstākais kontroles režīms vai dati ietver sensitīvus personas datus – jāpaaugstina uz 4. līmeni.
Ar autortiesībām aizsargāti darbi un to fragmenti (intelektuālā īpašuma objekti)	Atkarīgs	3. Paaugstinātas aizsardzības dati	Grāmatas, brošūras, lekciju materiāli; datorprogrammas; audiovizuāli darbi; fotogrāfijas; zīmējumi, gleznas, grafikas darbi; dizaina darbi; arhitektūras skices un projekti; kartes un plāni.	Šādi materiāli ir aizsargāti ar autortiesībām, to kopēšana, publicēšana vai izplatīšana var būt ierobežota ar likumu un/vai licenci.	Ja datu avots/līgums nosaka visaugstāko režīmu vai materiāli ir īpaši jutīgi pēc satura/komerciālās vērtības – jāpaaugstina uz 4. līmeni.

Datu veids / kategorija pētniecībā	Vai tie iekļauj personas datus?	Piedāvātais aizsardzības līmenis	Piemēri pētījumos	Kāpēc šis līmenis tiek piedāvāts?	Gadījumi, kad aizsardzības līmenis jāpaaugstina
Īpaši jutīgi tehnoloģiskie materiāli (ar augstu komerciālu vērtību)	Atkarīgs	4. Īpaši aizsargājamie dati	Nepublicēti tehniskie risinājumi; prototipu apraksti; tehnoloģiski "kodola" risinājumi; dati, kuru izpaušana var ietekmēt konkurenci vai stratēģiju.	Neatļauta izpaušana var radīt smagu kaitējumu institucionālām vai komerciālām interesēm.	Ja datu avots tieši nosaka visaugstāko aizsardzības režīmu vai izpaušana var radīt smagas sekas – jāpiemēro 4. līmenis.
Sensitīvie (īpašo kategoriju) personas dati	Jā	4. Īpaši aizsargājamie dati	Rase/etniskā izcelsme; politiskie uzskati; reliģiskā/filozofiskā pārliecība; dalība arodbiedrībā; dati par dzimumdzīvi vai seksuālo orientāciju.	Šie dati ir īpaši jutīgi, neatļauta piekļuve vai izpaušana var radīt smagu kaitējumu personai.	Šai datu grupai aizsardzības līmenis parasti nav pazemināms. Ja šādi dati ir pētījumā, jāpiemēro 4. līmenis.
Veselības dati (sensitīvo datu apakštips)	Jā	4. Īpaši aizsargājamie dati	Pacienta medicīniskā dokumentācija; diagnozes; ārstēšanas dati; medicīniskās fotogrāfijas; informācija par uzturu; slimnīcas kartes.	Veselības dati ir īpaši jutīgi, un to izpaušana var radīt īpaši smagas sekas personai.	Aizsardzības līmenis saglabājams 4. neatkarīgi no apjoma; ja dati tiek kombinēti ar citiem avotiem, risks pieaug.
Ģenētiskie dati un biometriskie dati (sensitīvo datu apakštips)	Jā	4. Īpaši aizsargājamie dati	Ģenētiskais materiāls; biometriskie dati; bioloģiskās pazīmes; identifikācijai izmantotas biometriskas pazīmes.	Šie dati cieši saistīti ar identitāti un ir grūti "atcelt", ja tie noplūst.	Aizsardzības līmenis saglabājams 4. neatkarīgi no apjoma; ja dati tiek kombinēti ar citiem avotiem, risks pieaug.
Sodāmības dati vai informācija par krimināllizmeklēšanām (augsta riska personas dati)	Jā	4. Īpaši aizsargājamie dati	Sodāmības dati; informācija par kriminālprocesu; saistīti ieraksti, kas var ietekmēt personas tiesisko stāvokli vai reputāciju.	Šāda informācija pētniecībā ir īpaši jutīga un rada augstu risku datu subjekta tiesībām.	Aizsardzības līmenis saglabājams 4. neatkarīgi no apjoma; ja dati tiek kombinēti ar citiem avotiem, risks pieaug.
Dati par bērniem vai citām ievainojamām personu grupām	Jā	3. Paaugstinātas aizsardzības dati	Bērnu vai pusaudžu dati; ievainojamu pieaugušo dati; dalībnieku grupas, kurām objektīvi nepieciešama pastiprināta aizsardzība.	Dati attiecas uz personām, kuru tiesības un intereses ir īpaši aizsargājamas, un neatļauta izpaušana var radīt nesamērīgi smagu kaitējumu.	Piemērojama pastiprināta piesardzība. Ja dati ietver sensitīvus datus vai ja datu apjoms, detalizācijas pakāpe vai apstrādes konteksts rada paaugstinātu risku datu

Datu veids / kategorija pētniecībā	Vai tie iekļauj personas datus?	Piedāvātais aizsardzības līmenis	Piemēri pētījumos	Kāpēc šis līmenis tiek piedāvāts?	Gadījumi, kad aizsardzības līmenis jāpaaugstina
					subjektam – jāpaaugstina uz 4. līmeni.
Sasaistītas vai kombinētas datu kopas no vairākiem avotiem, kas palielina iespēju noteikt personu	Jā	3. Paaugstinātas aizsardzības dati	Vairāku iestāžu dati kopā; datu kopas, kurās viens avots “atšifrē” otru.	Apvienošana var būtiski palielināt risku, ka persona kļūst atpazīstama, pat ja atsevišķi dati šķiet mazāk jutīgi.	Ja dati ietver sensitīvus datus vai ja datu apjoms, detalizācijas pakāpe vai apstrādes konteksts rada paaugstinātu risku datu subjektam – jāpaaugstina uz 4. līmeni.
Liela apjoma analītiskas datu kopas, ko izmanto personu profilēšanai, automatizētai lēmumu pieņemšanai vai novērošanai	Jā	4. Īpaši aizsargājamie dati	Detalizēti uzvedības vai lietojuma dati; ilgtermiņa novērošanas dati; analītika, kas ļauj izdarīt secinājumus par konkrētu personu.	Šādas datu kopas var radīt būtisku ietekmi uz personas tiesībām un interesēm, īpaši, ja tās izmanto ilgtermiņā vai kombinācijā ar citiem datiem.	Aizsardzības līmenis saglabājams 4., īpaši, ja analītika ir liela mēroga, ilgstoša vai balstīta uz vairāku datu avotu kombinēšanu.
Komercnoslēpumi (kā definēts likumā vai līgumā)	Atkarīgs	4. Īpaši aizsargājamie dati	Skices, dizaini, prototipi, ražošanas procesi, izgudrojumi, “know-how”, formulas/receptes, biznesa modeļi un stratēģija, cenu veidošanas politika, klientu/piegādātāju saraksti.	Šī informācija ir slepena un tai ir komerciāla vērtība; neatļauta izpaušana var radīt lielus zaudējumus.	Ja datu turētājs norāda, ka informācija ir komercnoslēpums, vai ja no satura izriet slepenība un komerciāla vērtība – jāpiemēro 4. līmenis.
Cita konfidenciāla informācija (ko datu avots nosaka par konfidenciālu, pat ja tā nav komercnoslēpums)	Atkarīgs	3. Paaugstinātas aizsardzības dati	Nepubliski iestāžu/uzņēmumu iekšējie materiāli, kuri nesatur komercnoslēpumu, bet datu avots pieprasa neizplatīt / līgumā noteikts ierobežojums.	Šādai informācijai var būt līgumiski ierobežojumi; pārkāpums var radīt atbildības riskus.	Ja informācija pēc satura ir ļoti jutīga (stratēģiska, drošības kontekstā) vai līgumā noteikts visaugstākais režīms – jāpaaugstina uz 4. līmeni.
Dati, kuriem datu avots vai līgums nosaka visaugstāko kontroles režīmu	Atkarīgs	4. Īpaši aizsargājamie dati	Jebkuri dati, par kuriem līgumā noteikts visaugstākais kontroles režīms	Līguma nosacījumi ir izšķiroši – tie nosaka, ka dati jāapstrādā ar visaugstāko aizsardzību.	Ja līgumā paredzēts visaugstākais režīms, aizsardzības līmenis nav pazemināms.

1. Līmenis – Atvērtie dati

Atvērtie dati ir dati, kurus var droši padarīt publiski pieejamus bez būtiska riska datu subjektiem, datu sniedzējiem, pētniekiem, sadarbības partneriem vai sabiedrības interesēm. Šajā līmenī ietilpst dati, kas nav personas dati, kā arī dati, kas ir pilnībā un neatgriezeniski anonimizēti tādā apmērā, ka atkārtota identificēšana nav saprātīgi iespējama.

Datu grupas īpašības:

Šī līmeņa dati ir piemēroti atklātai publicēšanai, atvērto datu repozitorijiem, plašai atkārtotai izmantošanai un zinātnisko rezultātu publiskai izplatīšanai. Datu atklāšana nerada būtisku juridisku, ētisku, komerciālu vai reputācijas risku.

Ja pastāv šaubas par anonimizācijas pilnīgumu vai ja dati kombinācijā ar citiem avotiem varētu ļaut identificēt personu vai citu aizsargājamu vienību, dati nav klasificējami kā atvērtie dati.

Raksturīgie datu veidi:

- Publiski pieejamas atvērtās datu kopas, kas nesatur identificējamus personas datus.
- Pilnībā anonimizētas pētniecības datu kopas, kurās atkārtotas identificēšanas risks ir novērsts.
- Publiski metadati, datu vārdnīcas, metodoloģiju apraksti un kods, kas neatklāj aizsargājamu saturu.
- Apkopotā statistika un kopsavilkuma rezultāti, kurus pamatoti nevar attiecināt uz indivīdiem vai aizsargātām vienībām.

2. Līmenis – Publiski nepieejami dati

Publiski nepieejami dati ir pētniecības dati, kas nav paredzēti publiskai izpaušanai, bet kuru neatļauta izpaušana nerada būtisku kaitējumu datu devējam, neizraisa nopietnas juridiskas sekas un neietver identificējamus personas datus, īpašu kategoriju personas datus, komerciāli jutīgu informāciju, līgumiski ierobežotus datus vai citus pielīdzināmus informācijas paveidus.

Datu grupas īpašības:

Šajā līmenī ietilpst pētniecības dati, kas savākti, novēroti vai izveidoti pētniecības projekta gaitā un tiek izmantoti analīzei, rezultātu iegūšanai vai secinājumu izdarīšanai, taču nav paredzēti publiskai pieejamībai. Šie dati pēc būtības ir zema riska privātuma, ētikas, komerciālā un drošības ziņā, tomēr tie ir aizsargājami no nepamatotas publiskas izpaušanas.

Ja datu izpaušana var radīt privātuma pārkāpumu, līgumisku atbildību, komerciālu zaudējumu vai būtisku reputācijas kaitējumu, dati jāvērtē kā augstāka aizsardzības līmeņa dati.

Raksturīgie datu veidi:

- Pētniecības gaitā radītas piezīmes, novērojumi un anotācijas, kas nesatur personas vai komerciāli jūtīgus datus.
- Nepublicētas darba datu kopas un starprezultāti, ja tie nesatur identificējamus personas datus un nav komerciāli, līgumiski vai intelektuālā īpašuma ziņā sensitīvi.
- Pētniecības procesā izmantoti mērījumi, teksts, attēli, koda fragmenti vai citi datu formāti, kas nav publiski izpaužami vismaz pētniecības laikā. Tai skaitā sintētiski veidoti vai paraugdati, kas tiek izmantoti pētniecības procesā, bet kas nav iegūti no reāliem aizsargājamiem ierakstiem un nerada atkārtotas identificēšanas risku.

3. Līmenis – Paaugstinātas aizsardzības dati

Dati, kuru neatļauta izpaušana, neatbilstoša apstrāde vai nepietiekami kontrolēta kopīgošana varētu radīt būtisku kaitējumu datu avotiem, pētniecības iestādēm, projekta partneriem vai datu subjektiem, taču parasti neietilpst visaugstākajā riska kategorijā. Šis līmenis aptver lielāko daļu komerciāli jutīgu, līgumiski ierobežotu, ar intelektuālā īpašuma tiesībām saistītu un identificējamu personas pētniecības datu, ja to apstrāde vēl neatbilst īpaši aizsargājamo datu līmenim.

Datu grupas īpašības:

Šī līmeņa dati nav publiski un tiem jābūt pieejamiem tikai autorizētiem lietotājiem ar pamatotu pētniecisku nepieciešamību. Līmenis aptver lielāko daļu ikdienā sastopamo aizsargājamo pētniecības datu, tostarp datus, kuri ir regulēti, līgumiski ierobežoti vai saistīti ar privātuma, komercnoslēpuma vai intelektuālā īpašuma aizsardzību.

Ja datu neatļauta izpaušana, kombinēšana vai atkārtota identificēšana var radīt nopietnu kaitējumu personu drošībai, veselībai, tiesībām vai sabiedrības interesēm, vai arī ja dati ietver īpašu kategoriju personas datus augsta riska kontekstā, tie jāvērtē kā īpaši aizsargājami dati.

Raksturīgie datu veidi:

- Interviju dati, aptauju dati un citi pētniecības ieraksti, kas satur tiešus vai netiešus personas identifikatorus.
- Pseidonimizēti personas dati, ja pastāv saprātīgi iespējams atkārtotas identificēšanas risks.
- Nepubliski uzņēmējdarbības dati, operatīvie dati un trešo pušu dati, kas nodoti pētniecībai saskaņā ar līgumu.
- Ar intelektuālā īpašuma tiesībām saistīti dati, nepublicēti tehniskie risinājumi vai pētniecības rezultāti ar komerciālu vērtību.
- Parasti identificējami personas dati, tostarp interviju dati, aptauju dati ar identifikatoriem un ar kontaktinformāciju saistīti pētniecības ieraksti.
- Līgumiski ierobežotas trešo pušu datu kopas, kurām nepieciešama kontrolēta apstrāde.

4. Līmenis - Īpaši aizsargājami dati

Dati, kuru neatļauta izpaušana, nepareiza izmantošana, kombinēšana vai atkārtota identificēšana var radīt nopietnu vai smagu kaitējumu datu subjektiem, datu sniedzējiem, institucionālajām interesēm vai sabiedrības interesēm. Šis ir augstākais aizsardzības līmenis, kam nepieciešami visstingrākie organizatoriskie, tehniskie un piekļuves kontroles pasākumi.

Datu grupas īpašības:

Šajā līmenī ietilpst augsta riska personas dati, augstas sensitivitātes komerciālie dati un citi datu kopumi, kuru ļaunprātīga izmantošana vai noplūde var izraisīt būtisku privātuma, ētisku, juridisku, stratēģisku vai sabiedrisku ietekmi. Datu sensitivitāti šajā līmenī bieži nosaka ne tikai paši dati, bet arī to kombinēšana ar citiem avotiem.

Dati klasificējami kā īpaši aizsargājami, ja pastāv augsta varbūtība, ka neatļauta piekļuve, identifikācija, noplūde vai sekundāra izmantošana var radīt nopietnu kaitējumu indivīdiem vai būtiski apdraudēt institucionālās, komerciālās vai sabiedrības intereses.

Raksturīgie datu veidi:

- Īpašu kategoriju personas dati, tostarp veselības dati, ģenētiskie dati, biometriskie dati vai dati, kas atklāj īpaši sensitīvas personiskas pazīmes.
- Ļoti jutīgi identificējami personu dati, it īpaši, ja to atklāšana var radīt nopietnu kaitējumu personām.

- Sasaistītas vai kombinētas datu kopas, kur apvienošana būtiski palielina identificēšanas risku.
- Dati par neaizsargātām personām, bērniem vai ētiski jūtīgām grupām augsta riska pētniecības kontekstos.
- Liela mēroga vai augsta riska analītiskās datu kopas, ko izmanto personu profilēšanai automatizētai lēmumu pieņemšanai vai novērošanai.
- Augstas sensitivitātes komercnoslēpumi, tehnoloģiskie vai īpašumtiesībās aizsargāti dati, kuru izpaušana var radīt smagas stratēģiskas, konkurences vai sabiedrības interešu sekas.
- Citi augsti aizsargāti dati, kuru apstrādei datu sniedzēji vai līgumiskās vienošanās nosaka visaugstākos kontroles mehānismus

2. Datu pārvaldības pamatprincipi

2.1 Vispārīgie pamatnosacījumi aizsargājamo datu izmantošanai

Lai efektīvāk organizētu aizsargājamo datu izmantošanu un pārvaldību, institūcijām un pētniekiem ieteicams ievērot arī šādus pārvaldības un drošības pamatprincipus, kas piemērojami neatkarīgi no konkrētā tehnoloģiskā risinājuma vai pētniecības dzīves cikla posma. Šīs norādes attiecas uz datiem, kas ietilpst 2., 3., 4. aizsardzības līmenī.

- **Datus drīkst izmantot tikai apstiprinātam un dokumentētam pētniecības mērķim.** Pirms datu saņemšanas vai izmantošanas jābūt skaidri noteiktam, kādam nolūkam dati tiks izmantoti, kas par to ir atbildīgs un kādā vidē apstrāde notiks.
- **Datu pārvaldība jāīsteno atbilstoši FAIR principiem.** Datu pārvaldība jāīsteno ievērojot FAIR principus tādā līmenī, kas nosedz datu aizsardzības, konfidencialitātes, līgumiskās un normatīvās prasības. Aizsargājamu datu gadījumā pieejamība un atkārtota izmantošana nedrīkst mazināt nepieciešamo aizsardzības līmeni.
- **Jāpiemēro datu minimizācijas princips.** Jāizmanto tikai konkrētajam pētījumam nepieciešamais datu apjoms, detalizācijas pakāpe un identificējamības līmenis. Ja pētniecības mērķi iespējams sasniegt ar mazāk sensitīviem datiem, priekšroka dodama anonimizētiem, pseidonimizētiem, agregētiem vai citādi mazāk aizsargājamiem datiem.
- **Piekļuve datiem piešķirama tikai autorizētām personām ar pamatotu nepieciešamību.** Piekļuves tiesībām jābalstās uz nepieciešamība zināt un vismazāk piešķirto piekļuves principu. Koplietotu kontu, kopīgu paroļu vai citu nepersonificētu piekļuves risinājumu izmantošana nav pieļaujama.
- **Jānodrošina piekļuves un darbību žurnalēšana.** Jābūt iespējai noteikt, kura persona ir piekļuvusi datiem, kad piekļuve notikusi un kādas darbības ar datiem veiktas. Lietotāju piekļuves, darbības un drošības notikumi ne tikai jāžurnalē, bet arī aktīvi jāuzrauga. Jābūt noteiktai kārtībai drošības incidentu identificēšanai, eskalācijai, izmeklēšanai un seku novēršanai, kā arī atbildīgajām personām šajā procesā.
- **Aizsargājamu datu glabāšanai, apstrādei un kopīgošanai priekšroka jādod institūcijas nodrošinātiem vai saskaņotiem risinājumiem**. Personīgu vai citu neinstitucionālu risinājumu izmantošana pieļaujama tikai izņēmuma gadījumos pēc iepriekšējas izvērtēšanas un saskaņošanas.
- **Datu glabāšanā un pārsūtīšanā jāizmanto šifrēšana.** Šifrēšana palīdz mazināt risku, ka dati kļūst pieejami nepiemērotajām personām gadījumos, kad notiek datu nodošana starp sistēmām vai rodas datu noplūde uzglabāšanas laikā.
- **Datu pārvaldības procesā jāievēro datu devēja vai normatīvā regulējuma noteiktie papildu ierobežojumi.** Ja datu izmantošanai tiek noteikti papildu nosacījumi, piemēram, attiecībā uz izmantošanas mērķi, lietotāju loku vai apstrādes vidi, tie jāievēro papildus vispārējām datu pārvaldības prasībām.
- **Jānosaka datu glabāšanas termiņš, pārskatīšanas kārtība un dzēšanas vai arhivēšanas nosacījumi.** Dati jāglabā tikai tik ilgi, cik tas nepieciešams pētniecības mērķa sasniegšanai vai cik to nosaka piemērojamās datu devēja prasības vai normatīvais regulējums. Pēc šī termiņa dati ir neatgriezeniski jādzēš vai jāarhivē kontrolētā kārtībā, kā to pieprasa normatīvais regulējums, noslēgtais līgums vai pētniecības plāns.

Paaugstinoties datu aizsardzības līmenim, datu pārvaldības procesā jāņem vērā papildu drošības apsvērumi. Tie papildina iepriekš noteiktos datu pārvaldības principus un palīdz labāk mazināt ar datu apstrādi saistītos drošības riskus. Šīs papildu prasības piemērojamas, sākot ar 3. un 4. līmeni.

- **Īpaši aizsargājamu datu izmantošana ir pieļaujama, ja tā ir skaidri pamatota.** Šādu datu izmantošana tiek veikta tikai gadījumos, kad pētniecības mērķi nav sasniedzami ar mazāk sensitīviem, mazāk detalizētiem, anonimizētiem, pseidonimizētiem vai agregētiem datiem.
- **Īpaši aizsargājamu datu apstrādei jānotiek īpaši kontrolētā vidē.** Atkarībā no konkrētā gadījuma tā var būt droša apstrādes vide vai cita līdzvērtīgi kontrolēta vide ar pastiprinātiem tehniskajiem un organizatoriskajiem aizsardzības pasākumiem.
- **Īpaši aizsargātiem datiem jānodrošina stingra piekļuves kontrole.** Lietotāju lokam jābūt maksimāli ierobežotam, un piekļuves tiesībām jāatbilst tikai konkrētajai nepieciešamībai. Jāizmanto daudzfaktoru autentifikācija, un ja piekļuve tiek organizēta institūcijas infrastruktūrai, jāparedz papildu drošības mehānismi, kā, piemēram, VPN.
- **Jābūt iespējai ierobežot datu iznešanas iespējas.** Datu kopēšanai, lejupielādei vai cita veida iznešana no kontrolētās vides jābūt tehniski pārvaldītai un jābūt iespējai to ierobežot.

Pamatprincipu ieviešanu ieteicams veikt samērīgi, izvēloties tādus drošības un pārvaldības pasākumus, kas atbilst konkrētā pētījuma riskiem, datu aizsardzības līmenim un institūcijas organizatoriskajām un tehnoloģiskajām iespējām.
Izvēlētajai pieejai jābūt pamatotai un dokumentētai, īpaši gadījumos, kad kāda kontrole tiek ieviesta pakāpeniski vai aizstāta ar pagaidu aizstājošiem pasākumiem. Vienlaikus 3. un īpaši 4. līmeņa datiem nedrīkst pazemināt minimāli nepieciešamo aizsardzības līmeni tikai ērtības vai resursu ierobežojumu dēļ.

2.2 Lomas datu pārvaldības procesā

Aizsargājamu datu izmantošana pētniecībā nav tikai tehnisks jautājums. Lai datu izmantošana būtu droša un efektīvi īstenojama, ieteicams jau pirms datu saņemšanas skaidri noteikt, kas pieņem lēmumus, kas ir atbildīgs par datu izmantošanu, kas uztur tehnisko vidi un kas uzrauga atbilstību noteiktajiem nosacījumiem. Skaidrs lomu sadalījums samazina neskaidrības starp pētniekiem, institūcijas atbalsta funkcijām un datu devējiem.

Šī dokumenta mērķis nav noteikt vienu universālu organizatorisko modeli visām institūcijām. Tā vietā ieteicams katram projektam vai datu izmantošanas gadījumam noteikt praktiski saprotamu atbildības modeli, kurā ir skaidri zināms vismaz:

- Kā tiek pamatota datu izmantošanas vajadzība;
- Kā tiek apstiprināta datu izmantošana un piekļuve;
- Kā tiek nodrošināta vai apstiprināta tehnoloģiskā vide;
- Kā tiek uzraudzīta datu pārvaldība pret normatīvajām, līgumiskajām un institucionālajām prasībām;
- Kā tiek pieņemti lēmumi par izmaiņām projektā, piemēram, ja mainās komanda, datu apjoms, izmantotie rīki vai paredzētā apstrādes vide.

Datu lietotājs (turpmāk - pētnieks) ir atbildīgs par datu izmantošanu tikai apstiprinātajam pētniecības mērķim, noteiktajā apjomā un paredzētajā vidē. Ieteicams, lai pētnieks izmantotu tikai saskaņotus rīkus un risinājumus, nepārsniegtu piešķirtās piekļuves tiesības un savlaicīgi informētu par nepieciešamām izmaiņām projektā, piemēram, ja tiek plānots izmantot papildu datus, citus rīkus vai citu apstrādes vidi.

Piesaistīts ārējais pētnieks vai speciālists ir ārpus institūcijas piesaistīta persona, kurš iesaistās konkrēta pētniecības projekta vai uzdevuma īstenošanā uz līguma pamata.

Datu devējs ir persona, institūcija, organizācija vai cita puse, kas pētniecības vajadzībām sniedz, nodod, dara pieejamus vai citādi ļauj izmantot datus. Tas var būt gan datu turētājs vai organizācija, kas nodod datu kopu faila, datubāzes, reģistra vai informācijas sistēmas veidā, gan arī pētījuma dalībnieks, kurš sniedz savus datus intervijā, aptaujā, novērojumā vai citā pētniecības procesā.

Datu devējs atbilstoši savai lomai nosaka, saskaņo vai tiek informēts par datu izmantošanas nosacījumiem, tostarp par izmantošanas mērķi, lietotāju loku, apstrādes vidi, glabāšanas termiņiem, publicēšanas ierobežojumiem un citiem drošības, konfidencialitātes vai ētikas nosacījumiem. Ja dati tiek nodoti ar īpašiem ierobežojumiem, ieteicams jau sākotnēji vienoties, kuras izmaiņas projekta gaitā datu lietotājs var pieņemt patstāvīgi un kuras jāsaskaņo ar datu devēju atkārtoti.

Pētniecības institūcija (turpmāk – institūcija) nodrošina datu pārvaldības pamata ietvaru un atbalsta funkcijas drošai datu izmantošanai. Praksē tas ietver piemērotas tehniskās vides nodrošināšanu vai izvērtēšanu, atbalstu atbilstības un datu aizsardzības jautājumos, kā arī iekšējās kārtības noteikšanu attiecībā uz pieļaujamo datu pārvaldības praksi. Šajā dokumentā institūcija saprotama kā organizācija, kurā darbojas konkrētais pētnieks (visbiežāk sastopamais veids - zinātniskās institūcijas, tostarp augstākās izglītības iestādes). Institūcija pētniekiem visbiežāk nodrošina šāda veida atbalstu:

Datu kurators – konsultē pētniekus par pētniecības datu pārvaldību, tostarp datu dzīves cikla plānošanu, metadatiem, dokumentēšanu, FAIR principu piemērošanu, repozitoriju izvēli un praktisku datu sagatavošanu glabāšanai, kopīgošanai vai publicēšanai. Datu kurators neaizstāj datu aizsardzības speciālistu, juridisko atbalstu, kiberdrošības speciālistu vai IT sistēmas īpašnieku. Ja jautājums prasa juridisku, personas datu aizsardzības vai tehniskās drošības izvērtējumu, datu kurators palīdz to virzīt attiecīgajai atbalsta funkcijai.

IT atbalsts – nodrošina tehnisko pamatu darbam ar datiem, programmatūru un digitālajiem rīkiem pētniecības procesā. IT atbalsta speciālisti palīdz pētniekiem izvēlēties un uzturēt drošus un uzticamus IT risinājumus, kā arī nodrošina piekļuvi datu pārvaldības tehnoloģiskajai infrastruktūrai.

Datu aizsardzības speciālists – konsultē par juridiskajiem aspektiem tieši kontekstā ar personas datu aizsardzību, nodrošinot, ka pētniecības procesā personas dati, tostarp sensitīvie personas dati, tiek apstrādāti likumīgi un droši, atbilstoši normatīvajam regulējumam kā VDAR.

Juridiskais atbalsts – atbalsta pētniekus, nodrošinot, ka pētniecības projektā datu pārvaldība tiek īstenota atbilstoši noteiktajām līgumiskajām saistībām un intelektuālā īpašuma prasībām. Juridiskie speciālisti konsultē par datu izmantošanas tiesībām, līgumiem, licencēm, sadarbības nosacījumiem, kā arī palīdz identificēt un mazināt juridiskos riskus jau projekta plānošanas posmā.

Praksē aizsargājamu datu nodošana pētniecībai visbiežāk notiek ar institūciju kā formālo saņēmēju, nevis ar individuālu pētnieku.

No datu devēja puses tā ir drošāka un uzticamāka pieeja. Šī iemesla dēļ institūcija ir iesaistīta arī tajā, lai nodrošinātu, ka dati tiek pārvaldīti droši, pārskatāmi un atbilstoši noteiktajiem datu devēja nosacījumiem un institūcijas pārvaldības kārtībai.

Pētnieks var patstāvīgi organizēt darbu ar 1. un 2. līmeņa datiem, ja tiek izmantoti institūcijas apstiprināti rīki un ievērotas šajā dokumentā noteiktās prasības. Tomēr papildu konsultācijas vai izvērtējumu būtu nepieciešams veikt šādos gadījumos:

Datu kurators jāiesaista, ja:

- datu klasifikācija nav viennozīmīga;
- ir šaubas par anonimizācijas vai pseidonimizācijas pietiekamību;
- dažādu datu kopu apvienošana var mainīt datu aizsardzības līmeni un to ir nepieciešams padziļinātāk izvērtēt.

Datu aizsardzības speciālists jāiesaista, ja:

- dati ietver personas datus;
- dati ietver īpašu kategoriju personas datus;
- datu izmantošana var radīt paaugstinātu risku datu devēju tiesībām vai interesēm.

Juridiskais atbalsts jāiesaista, ja datu izmantošanu ierobežo:

- līguma nosacījumi;
- intelektuālā īpašuma tiesības;
- komerciāla sensitivitāte;
- konfidencialitātes prasības.

IT atbalsts jāiesaista jautājumos par:

- rīku vai platformu piemērotību;
- drošas apstrādes vides izvēli;
- tehniskās konfigurācijas vai piekļuves risinājumu atbilstību.

3. un 4. līmeņa datu izmantošanai, kā arī jaunām vai būtiski mainītām augsta riska apstrādes darbībām, pirms datu saņemšanas vai apstrādes uzsākšanas ieteicams paredzēt formālu izvērtēšanu un apstiprināšanas ciklu institūcijā.

2.3 Datu piekļuves tiesību organizēšana un kontrole

Piekļuves piešķiršanas pamatprincipi

Piekļuve aizsargātiem pētniecības datiem jāpiešķir tikai identificētiem lietotājiem un tikai tādā apjomā, kas nepieciešams konkrētā pētniecības uzdevuma veikšanai. Piekļuvei jābūt piesaistītai lietotāja lomai, projekta vajadzībai un datu izmantošanas nosacījumiem.

Piešķirot piekļuves tiesības, jāņem vērā vismaz šādi principi:

- piekļuve tiek piešķirta tikai apstiprinātam lietotājam;
- piekļuve tiek ierobežota līdz konkrētai datu kopai vai darba videi;
- lietotājam tiek piešķirtas tikai nepieciešamās darbības, piemēram, apskatīšana, komentēšana, rediģēšana vai lejupielāde;
- piekļuvei jābūt ar noteiktu pamatojumu un, ja iespējams, ar noteiktu termiņu;
- nevajadzīgas, neizmantotas vai pārmērīgas tiesības ir jāatsauc.

Piekļuves organizēšanā svarīgi ir ne tikai izlemt, vai piekļuve ir vajadzīga, bet arī noteikt, cik plaša šī piekļuve drīkst būt. Aizsargātiem pētniecības datiem jāpiemēro tāds piekļuves modelis, kas samazina nevajadzīgu datu pieejamību un ierobežo kļūdas vai neatļautas izmantošanas risku. Praksē tas nozīmē, ka piekļuve var tikt ierobežota:

- pēc datu kopas vai projekta;

- pēc lietotāja lomas vai funkcijas;
- pēc pieļautajām darbībām;
- pēc termiņa;
- pēc izmantotās sistēmas piekļuvei.

Ja iespējams, piekļuves tiesības piešķir pēc lomām vai iepriekš definētām piekļuves grupām, nevis katru gadījumu konfigurējot pilnīgi individuāli. Tas atvieglo pārvaldību un samazina kļūdu risku, kas var rasties piekļuves pārvaldības procesā.

Piekļuves izmaiņas un atcelšana

Piekļuves tiesībām jābūt pārvaldītām visā to dzīves ciklā. Tās ir periodiski jāpārskata, lai pārliecinātos, ka tās joprojām atbilst aktuālajai darba vajadzībai un nav saglabājušās ilgāk, nekā nepieciešams. Tas nozīmē, ka tiesības ne tikai piešķir, bet arī savlaicīgi maina vai atceļ, ja mainās lietotāja pienākumi, projekta tvērums vai datu izmantošanas pamats.

Piekļuve ir jāpārskata un vajadzības gadījumā jāatceļ vismaz šādos gadījumos:

- lietotājs vairs nepiedalās projektā;
- mainās lietotāja loma vai darba pienākumi;
- projekts ir noslēdzies vai datu izmantošanas periods ir beidzies;
- tiek konstatēts, ka piešķirtās tiesības ir pārmērīgas vai vairs nav pamatotas;
- lietotāja konts ilgstoši netiek izmantots.

Piekļuves dokumentēšana un izsekojamība

Lai piekļuves tiesību organizēšana būtu pārbaudāma, organizācijai jāspēj izsekot, kam piekļuve ir piešķirta, uz kāda pamata tā piešķirta un kad tā pārskatīta vai atcelta.

Minimāli būtu jāfiksē:

- piekļuves pieprasījums un tā pamatojums;
- piekļuves apstiprinātājs un apstiprinājuma datums;
- piešķirto tiesību apjoms un termiņš;
- veikto izmaiņu vai atcelšanas fakts.

Rīcība neatbilstošu tiesību gadījumā

Ja tiek konstatēts, ka lietotājam piešķirtas nepamatotas, pārmērīgas vai kļūdainas piekļuves tiesības, tās nekavējoties jākoriģē vai jāatceļ. Vienlaikus jāizvērtē, vai neatbilstošā piekļuve nav radījusi ar datiem saistītu incidentu un vai nav nepieciešami papildu pasākumi.

Šādos gadījumos ieteicams:

- nekavējoties samazināt vai atcelt neatbilstošās tiesības;
- fiksēt konstatēto neatbilstību un veiktās darbības;
- izvērtēt cēloni, piemēram, kļūdu procesā vai nepietiekamu pārskatīšanu;
- ja nepieciešams, piemērot incidentu pārvaldības kārtību.

2.4 Rīcība datu noplūdes vai drošības incidenta gadījumā

Šajā nodaļā tiek piedāvāta rīcības kārtība gadījumiem, kad aizsargāti pētniecības dati var būt kļuvuši pieejami neatļautām personām, nozaudēti, nepareizi nosūtīti, neatļauti izmainīti vai izmantoti neatļautā vidē vai ārpus apstiprinātā nolūka. Šādas situācijas ir jāuzskata par ar datiem saistītiem incidentiem, un uz tām jāreaģē nekavējoties, lai ierobežotu ietekmi uz datiem, pētniecības projektu un datu devēja interesēm.

Kad piemērojama šī kārtība

Šī kārtība jāpiemēro, ja ir aizdomas vai ir zināms, ka aizsargāti pētniecības dati:

- Nosūtīti nepareizam saņēmējam;
- Saglabāti vai augšupielādēti neatļautā vietā;
- Kļuvuši pieejami personām, kurām nav piešķirtas atbilstošas piekļuves tiesības;
- Nozaudēti, dzēsti vai izmainīti bez atļaujas;
- Izmantoti rīkā, pakalpojumā vai darba vidē, kas konkrētajam datu veidam vai projektam nav apstiprināti.

Sākotnējā rīcība

Personai, kura incidentu pamana vai par to uzzina, nekavējoties jāveic šādas darbības:

- Jāpārtrauc turpmāka datu kopīgošana, pārsūtīšana vai apstrāde attiecīgajā failā, sistēmā vai pakalpojumā;
- Jāizvairās no liekām izmaiņām datos, failos vai sistēmā, lai netiktu zaudēta informācija par incidenta apstākļiem;
- Jāsaglabā pieejamā informācija par notikumu, tostarp laiks, izmantotā sistēma, skartā datu kopa, iespējamie saņēmēji un citas zināmās detaļas;
- Ja tas nepieciešams turpmāka kaitējuma ierobežošanai, jāaptur piekļuve datiem, vienlaikus cenšoties nesabojāt informāciju, kas vajadzīga incidenta izvērtēšanai;
- Nekavējoties jāziņo atbildīgajai personai par datu drošību un IT atbalstam.

Ziņošanas kārtība

Par incidentu jāziņo organizācijas noteiktajā kārtībā. Vismaz jāinformē projekta atbildīgā persona vai datu kopas atbildīgais, kā arī IT atbalsts, ja incidents saistīts ar sistēmu, kontu, piekļuvi vai datu glabāšanas vidi. Ja incidents var skart aizsargātās datu kopas vai datu devējam dotās saistības, jāiesaista arī par datu aizsardzību vai līgumisko atbilstību atbildīgā funkcija.

Sākotnējais izvērtējums

Pēc ziņojuma saņemšanas atbildīgajām pusēm pēc iespējas ātri jāizvērtē incidenta būtība un iespējamā ietekme. Izvērtējumā vismaz jānosaka, kāda veida dati ir skarti, vai tie ļauj tieši vai netieši identificēt personas vai citus aizsargājamus objektus, kāda ir incidenta ietekme, kam dati varēja kļūt pieejami un vai datu izmantošanu konkrētajā projektā drīkst turpināt bez papildu ierobežojumiem

Tūlītēji veicamie pasākumi

Ja incidents apstiprinās, jāveic samērīgi pasākumi, lai ierobežotu tā ietekmi. Atkarībā no situācijas tas var ietvert neatļautas kopīgošanas atsaukšanu, piekļuves tiesību vai kontu apturēšanu, paroļu vai piekļuves atslēgu nomaiņu, kā arī attiecīgo žurnālfailu, ziņojumu, ekrānuzņēmumu un citas informācijas saglabāšanu turpmākai izvērtēšanai. Vienlaikus jāpieņem lēmums, vai datu izmantošana uz laiku jāpārtrauc, jāierobežo vai drīkst turpināties tikai ar papildu drošības pasākumiem.

Ja to paredz datu izmantošanas nosacījumi, līgumiskās saistības vai incidenta raksturs, organizācijai jāinformē arī datu turētājs vai citas iesaistītās puses saskaņā ar noteikto kārtību.

Rīcība pēc incidenta

Pēc incidenta jāizvērtē, vai nepieciešamas izmaiņas piekļuves tiesībās, darba organizācijā, izmantotajos rīkos, apmācībā vai datu koplietošanas nosacījumos. Ja incidents parāda, ka konkrēta prakse, sistēma vai pakalpojums nav pietiekami drošs aizsargātu pētniecības datu apstrādei, tā izmantošana jāpārskata, jāierobežo vai jāpārtrauc.

3. Datu pārvaldība pētniecības dzīves ciklā

Datu izmantošana pētniecībā ir jāvērtē ne tikai pēc datu veida vai to aizsardzības līmeņa, bet arī pēc tā, kurā pētniecības dzīves cikla posmā dati atrodas un kā tie konkrētajā brīdī tiek izmantoti. Šī iemesla dēļ, viens no ērtākajiem veidiem ir sadalīšana pa galvenajiem datu pārvaldības dzīves cikla posmiem. Šāds sadalījums ļauj identificēt un noteikt skaidras vajadzības katram posmam, kuros aizsargājamie dati rada atšķirīgus riskus un prasa atšķirīgus kontroles pasākumus. Tajā pat laikā katrs no šiem posmiem ietver atšķirīgus tehnoloģiskos izaicinājumus un pielietojamos risinājumus.

Rekomendāciju struktūra balstās uz trim datu pamatstāvokļiem, kas raksturo vajadzības visā dzīves ciklā:

- dati pārsūtīšanas laikā *(angļu val. data in transit)*,
- dati glabāšanā *(angļu val. data at rest)*,
- dati apstrādē vai izmantošanā *(angļu val. data in use)*.

Pārsūtīšanas posmā galvenais uzsvars tiek vērsts uz drošiem nodošanas kanāliem, lai samazinātu risku, ka dati noplūst pārnešanas posmā.

Datu glabāšanas posmā būtiska ir atbilstošas tehnoloģiskās vides izvēle, piekļuves tiesību pārvaldība, datu šifrēšana, rezerves kopēšana un uzglabāšanas termiņu ievērošana.

Datu apstrādes un izmantošanas posmā galvenais uzsvars tiek vērts par to, kur un kā dati tiek analizēti, kam ir piekļuve darba videi, vai tiek izmantoti atbilstoši tehniskie ierobežojumi.

Datu aizsardzības līmeņa piemērošana

Šajā nodaļā prasības tiek pielāgotas atbilstoši iepriekš definētajiem datu aizsardzības līmeņiem, jo vieni un tie paši risinājumi nav vienlīdz piemēroti visiem datu veidiem. Ņemot vērā, ka pētniecības procesā var tikt izmantota programmatūra ar ļoti plašu funkcionalitāti, atbilstoši konkrētā pētījuma vajadzībām, zemāk minētie produktu nosaukumi tiek sniegti kā piemēri, nevis ierobežots risinājumu saraksts. Šajā gadījumā izšķirošais elements ir tas, vai risinājums ir institucionāli pārvaldīts vai apstiprināts, kā arī pareizi konfigurēts un piemērots attiecīgajam datu aizsardzības līmenim. Konkrētā risinājuma izmantošana ir pētnieka atbildība, tāpēc pirms tā izmantošanas ir nepieciešams veikt izvērtēšanu un, ja iespējams, konsultēties ar institūcijas tehnisko atbalstu.

Papildus šajā dokumentā piemērojamās prasības un rekomendācijas primāri tiek noteiktas pēc datu aizsargājamības līmeņa, nevis pēc datu tehniskā veida vai apjoma. Šāda pieeja izvēlēta tādēļ, ka svarīgākais faktors piemērojamo drošības prasību noteikšanā ir iespējamās sekas datu neatļautas izpaušanas, grozīšanas, zuduma vai neatbilstošas izmantošanas gadījumā.

Statiskas datu kopas, teksta, attēlu, audio vai video dati, lielapjoma dati un dinamiskie dati var atšķirties pēc tehnoloģiskajām vajadzībām, piemēram, nepieciešamās glabāšanas kapacitātes, skaitļošanas jaudas u.c., tomēr šīs atšķirības pašas par sevi nemaina pamatprasības attiecībā uz izvēlēto tehnoloģisko pieeju. Tādēļ tā vietā katram datu izmantošanas gadījumam vispirms nosaka datu aizsargājamības līmeni un pēc tam izvēlas konkrētajam datu veidam, apjomam un izmantošanas scenārijam piemērotu tehnoloģisko risinājumu, kuram piemēro attiecīgā aizsargājamības līmeņa kontroles.

Ja datu aizsardzības līmeņa izvēles brīdī pastāv šaubas par piemērojamo pieeju, tad ieteicams izvēlēties stingrāk kontrolētus risinājums, nevis ērtāko variantu.
Sākotnējā nenoteiktībā ieteicams izvēlēties drošāku ceļu arī, ja tas ir sarežģītāks, jo kļūdaini izvēlēts risinājums ar nepietiekamām drošības kontrolēm paaugstina saistītos datu noplūšanas riskus.

Datu sagatavošana pētniecībai

Pirms datu nodošanas izmantošanai pētniecības procesā jāizvērtē, vai dati ir sagatavoti atbilstoši pētniecības mērķim un tiem piemērojamajam aizsardzības līmenim. Datu sagatavošana šī dokumenta izpratnē ietver datu tīrīšanu, datu kopu apvienošanu, datu minimizāciju, tiešo identifikatoru izņemšanu, pseidonimizāciju, anonimizāciju, agregēšanu un pētniecībā izmantojamu darba datu kopu izveidošanu.

Datu sagatavošanas laikā jāievēro šādi nosacījumi:

- jāizmanto tikai tādi dati, datu lauki un detalizācijas pakāpe, kas nepieciešama apstiprinātajam pētniecības mērķim,
- datu tīrīšana, labošana, dublikātu dzēšana, formātu pārveidošana un citas būtiskas izmaiņas jāveic pārskatāmā un pamatotā veidā. Šis darbības ir jādokumentē,
- pirms datu kopu apvienošanas jāizvērtē, vai sasaistīšana nepalielina personas, komerciālās vai citas aizsargājamas informācijas identificēšanas vai izpaušanas risku,
- pseidonimizācijas gadījumā saiknes tabula vai pseidonimizācijas atslēga jāglabā atsevišķi no darba datu kopas un ar ierobežotu piekļuvi,
- anonimizāciju drīkst uzskatīt par pietiekamu tikai tad, ja ir izvērtēts, ka dati nav atkārtoti identificējami ar saprātīgi pieejamiem līdzekļiem,
- sagatavotajai darba datu kopai var tikt atkārtoti izvērtēts piemērojamais aizsardzības līmenis, jo apstrādātajai datu kopai, tas var paaugstināties vai samazināties,
- starprezultāti, atvasinātie dati un sagatavotās darba datu kopas joprojām jāuzskata par aizsargājamiem datiem, ja tie satur vai var atklāt sākotnēji aizsargājamu informāciju.

Sākotnējā datu kopa saglabā tai noteikto aizsardzības līmeni arī tad, ja no tās sagatavošanas procesā tiek veidoti atvasināti dati, starprezultāti vai publicēšanai paredzēti izvaddati. Piemēram, ja sākotnējā datu kopa ir klasificēta kā 4. līmeņa dati, tā parasti turpina būt 4. līmeņa dati visā tās glabāšanas un apstrādes laikā.

Sagatavotai atvasinātai datu kopai vai rezultātu kopai var noteikt zemāku aizsardzības līmeni tikai tad, ja dati ir pārveidoti tā, ka būtiski samazināts atkārtotas identificēšanas, konfidenciālas informācijas izpaušanas vai cita kaitējuma risks. Šāda pārveidošana var ietvert tiešo identifikatoru izņemšanu, datu agregēšanu, vērtību vispārināšanu, retu vai unikālu vērtību slēpšanu, anonimizāciju vai izvaddatu izpaušanas riska izvērtēšanu pirms to izmantošanas ārpus sākotnējās apstrādes vides. Šādos gadījumos zemāka aizsardzības līmeņa noteikšana nav automātiska. Pārklasificēšana ir atsevišķi jāizvērtē un jādokumentē, norādot, kādi pārveidošanas pasākumi veikti un kāpēc tie pietiekami samazina risku.

Turpmākajās sadaļās aprakstītās prasības piemērojamas gan sākotnēji saņemtajiem datiem, gan datu sagatavošanas rezultātā izveidotajām darba datu kopām, starprezultātiem un atvasinātajiem datiem.

3.1 Datu nodošana vai saņemšana

Datu nodošanas un saņemšanas posms ir viens no riska ziņā svarīgākajiem brīžiem visā pētniecības dzīves ciklā, jo tieši šajā posmā dati tiek pārvietoti starp iesaistītajām pusēm un to sistēmām. Praksē droša nodošana nozīmē ne tikai drošu tehnisko kanālu, bet arī skaidru vienošanos par to, kādi dati tiek nodoti, kam tie tiek nodoti, kādā formā, uz kādu vidi, uz cik ilgu laiku un ar kādiem ierobežojumiem.

Šo rekomendāciju izpratnē datu ieguve attiecas uz gadījumiem, kad dati tiek iegūti no datu avota informācijas sistēmām, aparatūras, mērierīcēm, sensoriem, datu nesējiem, aptaujām, intervijām, pētījuma dalībniekiem vai citiem sākotnējiem datu fiksēšanas avotiem.

Ja dati tiek iegūti no datu avota informācijas sistēmām, aparatūras vai tehniskiem datu nesējiem, datu izguvei un nodošanai izmantojama attiecīgajam aizsargājamības līmenim

piemērota datu pārraides metode, kas aprakstīta šajā sadaļā. Piemēram, 4. līmeņa datiem nav pieļaujama datu pārsūtīšana ar personīgiem e-pasta kontiem vai nekontrolētiem failu apmaiņas rīkiem.

Ja dati tiek iegūti tieši no datu devēja vai pētījuma dalībniekiem, piemēram, aptaujās, intervijās, mērījumos, audio vai video ierakstos, sākotnējai datu fiksēšanai, tad datu iegūšana ir vērtējama arī kā kombinēts datu apstrādes un glabāšanas posms, jo aptauju, interviju, ierakstu un līdzīgi rīki faktiski darbojas kā datu ievades, apstrādes un pagaidu glabāšanas vide. (Skatīt 3.2 un 3.3 nodaļu).

Pamatprincipi, kas attiecināmi uz visiem datu aizsardzības līmeņiem datu nodošanas posmā:

- Datu nodošanai jāizmanto risinājumi ar autentifikāciju, kas ir pārvaldīti un ir auditējami. Datu nodošanai ieteicams izmantot mehānismus, kas ļauj fiksēt nodošanas faktu vai vismaz praktiski pierādīt, kad, kam un kādā veidā dati nodoti, īpaši gadījumos, kad tiek nodoti 3. vai 4. līmeņa dati.
- Ja dati paredzēti glabāšanai vai apstrādei konkrētā institūcijas nodrošinātā vai apstiprinātā vidē, tie pēc iespējas jānogādā tieši šajā vidē, izvairoties no nevajadzīgām kopijām uz pētnieka ierīces vai citās starpvidēs.
- Ja nodošanas procesā tiek izmantotas pagaidu augšupielādes vides vai citi starpmehānismi, ieteicams nodrošināt, ka pēc datu saņemšanas šīs pagaidu kopijas tiek dzēstas vai piekļuve tām tiek slēgta.
- Ja dati tiek nodoti izmantojot ārēju pakalpojumu sniedzēju, ieteicams jau pirms nodošanas pārliecināties, ka izvēlētais risinājums atbilst datu devēja nosacījumiem, institūcijas prasībām un konkrētā datu aizsardzības līmeņa vajadzībām.
- Paaugstināta riska datu nodošanai jāizmanto šifrēta pārsūtīšana un droša atslēgu apmaiņa. Datus ieteicams pirms nosūtīšanas šifrēt, piemēram, ar PGP, un atslēgu apmaiņa jāveic atsevišķi no datu nodošanas kanāla.

Tabula 3 – Datu nodošanas vai saņemšanas pieejas izvēle

Tehnoloģiskā pieeja	Tipiskie risinājumi	Nosacījumi, kas jāievēro pārvaldot 2. līmeņa datus	Nosacījumi, kas jāievēro pārvaldot 3. līmeņa datus	Nosacījumi, kas jāievēro pārvaldot 4. līmeņa datus
Fiziski datu nesēji	USB zibatmiņa, ārējie diski.	Ieteicams tikai vienreizējai nodošanai vai gadījumos, kad nav pieejams piemērots tīkla risinājums. Pēc nodošanas pagaidu kopijas jādzēš.	Ieteicams tikai ar nosacījumiem gadījumos, kad nav pieejams piemērots tīkla risinājums vai datu devējs nodrošina nodošanu tikai šādā veidā. Lietot tikai šifrētu datu nesēju, jāierobežo pārvadāšana un pēc nodošanas dati jādzēš.	Nav ieteicams izmantot. Izņēmums tikai īpaši apstiprinātā procesā ar šifrēšanu, kontrolētu nodošanu un dzēšanu pēc pārneses.
Datu apmaiņa starp divām sistēmām	MFT risinājums, SFTP, WebDAV, API pārsūtīšana, piekļuve izmantojot pārvaldītu VPN.	Ieteicams datu apmaiņas veids, ja tiek lietota droša autentifikācija un šifrēta pārraide.	Ieteicams datu apmaiņas veids, ja tiek lietota droša autentifikācija un šifrēta pārraide.	Ieteicams tikai starp apstiprinātām, kontrolētām vidēm. Izvairīties no lokālas starpniekkopijas uz darbstacijas ārpus kontrolētas vides.
Institucionāli pārvaldīta datu glabāšanas vide	Institucionāli pārvaldīti risinājumi kā FileSender, Nextcloud, ownCloud u.c.	Ieteicams. Jābūt institucionāli pārvaldītam, ar piekļuves ierobežošanu konkrētiem lietotājiem vai grupām.	Ieteicams. Jābūt institucionāli pārvaldītam, ar piekļuves ierobežošanu konkrētiem lietotājiem vai grupām.	Nav ieteicams, pieļaujams tikai tad, ja risinājums faktiski darbojas kā kontrolēta nodošanas vārteja uz drošu vidi un neļauj brīvi izplatīt vai lokāli sinhronizēt datus.
Institucionāli pārvaldīta mākoņkrātuve	Institucionāli pārvaldīts Microsoft SharePoint, OneDrive, Google Drive.	Ieteicams. Jābūt institucionāli pārvaldītam, ar piekļuves ierobežošanu konkrētiem lietotājiem vai grupām.	Ieteicams. Jābūt institucionāli pārvaldītam, ar piekļuves ierobežošanu konkrētiem lietotājiem vai grupām.	Nav ieteicams, ja vien risinājums nav īpaši noteikts kā kontrolēta nodošanas vide 4. līmeņa datiem.
E-pasts	Institucionāli piešķirts e-pasta konts	Nav ieteicams kā pamatmetode. izmantot tikai neliela apjoma un zemāka riska nodošanai, ja nav piemērotāka risinājuma.	Neizmantot. 3. līmeņa datiem e-pasts nav paredzēts kā standarta datu apmaiņas vide.	Neizmantot

Tehnoloģiskā pieeja	Tipiskie risinājumi	Nosacījumi, kas jāievēro pārvaldot 2. līmeņa datus	Nosacījumi, kas jāievēro pārvaldot 3. līmeņa datus	Nosacījumi, kas jāievēro pārvaldot 4. līmeņa datus
		Pielikumiem jābūt šifrētiem, atslēga jānodod atsevišķi, un e-pasts nedrīkst kļūt par standarta datu apmaiņas vidi.		
Izvērtēti un saskaņoti ārējie mākoņpakalpojumi	Ārējie mākoņpakalpojumi, kas nav institūcijas pamatrisinājumi, piemēram, B2DROP, EOSC EU Node File Sync and Share, Azure Blob storage, AWS S3, GCP Cloud Storage	Ieteicams ar nosacījumiem. Izmantot tikai tad, ja risinājums ir izvērtēts un saskaņots konkrētajam lietojumam	Ieteicams ar nosacījumiem. Izmantot tikai tad, ja risinājums ir izvērtēts un saskaņots konkrētajam lietojumam	Pieļaujams ar nosacījumu, ka veikts institucionāls vai projekta līmeņa izvērtējums par datu drošību, datu rezidenci un datu glabāšanas nosacījumiem.
Personīgi vai citi personīgi pārvaldīti risinājumi	Personīgais e-pasts, personīgais OneDrive/Google Drive/Dropbox konts.	Neizmantot. Personīgi pārvaldīti risinājumi nav paredzēti pētniecības datu nodošanai un nenodrošina datu drošības līmeni.	Neizmantot	Neizmantot

Ieteicamā pieeja šī līmeņa datu apstrādei.
Pieļaujams ar nosacījumiem - nepieciešams izvērtējums un atbilstoši kontroles pasākumi.
Neizmantot šī līmeņa datiem. Atsevišķos gadījumos pieļaujams, piemēram, drošas apstrādes vides ietvaros.

3.2 Datu glabāšana

Datu glabāšana projekta laikā ir jāorganizē tā, lai dati būtu pieejami pētniecības darbam, vienlaikus saglabājot kontroli pār piekļuvi, datu kopiju veidošanos, aizsardzību pret neatļautu piekļuvi un aizsardzību pret nejaušu zudumu.

Praktiski tas nozīmē, ka glabāšanas risinājums jāizvēlas ne tikai pēc lietošanas ērtuma, bet arī pēc tā, vai tas nodrošina pietiekamu piekļuves kontroli, auditējamību, šifrēšanu, rezerves kopēšanu un atbilstību datu devēja vai iestādes noteiktajiem nosacījumiem.

Augstākiem datu aizsardzības līmeņiem glabāšanas videi jābūt stingrāk kontrolētai, un ir jāierobežo lokālu darba kopiju, sinhronizētu mapju un citu nekontrolētu datu kopiju veidošanās.

Pamatprincipi, kas attiecināmi uz visiem datu aizsardzības līmeņiem datu glabāšanas posmā:

- Projektam ieteicams noteikt vienu galveno glabāšanas vidi, kas tiek izmantota kā pamata datu glabāšanas vieta projekta laikā. Tas palīdz samazināt situācijas, kur vieni un tie paši dati paralēli glabājas vairākās vietās bez skaidras kontroles par to, kura kopija ir aktuālā un pārvaldītā
- Dati glabāšanai projekta laikā jādod priekšroka institucionāli pārvaldītā vai institucionāli saskaņotā vidē. Glabāšanas risinājumam jānodrošina piekļuves kontrole, lietotāju autentifikācija un iespēja ierobežot piekļuvi tikai iesaistītajām personām.
- Mākoņpakalpojumu izmantošana ir pieļaujama, ja tie ir izvērtēti un pārvaldīti atbilstoši drošības prasībām. Izvēloties mākoņpakalpojumu jāpārliecinās, ka datu apstrādes un glabāšanas vieta atbilst datu nodošanas līgumā, normatīvajā regulējumā vai citos saistošajos nosacījumos noteiktajām datu rezidences prasībām, tai skaitā prasībām datus apstrādāt tikai ES.
- Darba kopijas uz gala iekārtām vai citās pagaidu vietās ieteicams pieļaut tikai tad, ja tās ir pamatotas ar praktisku nepieciešamību un nepārvēršas par galveno glabāšanas risinājumu. Ieteicams izvairīties no situācijas, kur projekta faktiskā datu glabāšana notiek pētnieka klēpjdatorā vai sinhronizētā lokālā mapē.
- Izvēloties glabāšanas risinājumu, ieteicams vērtēt ne tikai tā lietošanas ērtumu, bet arī to, vai risinājums ļauj kontrolēt piekļuvi, versijas, rezerves kopēšanu un datu kopiju veidošanos uz citām ierīcēm vai pakalpojumiem.
- Glabāšanai jābūt aizsargātai arī pret nejaušu datu zudumu. Tas nozīmē, ka glabāšanas videi jānodrošina rezerves kopēšana, versiju vēsture vai citi atjaunošanas mehānismi, kas ir samērīgi pret datu kopu nozīmīgumu un aizsardzības līmeni.
- Ieteicams noteikt, cik ilgi dati un ar tiem saistītās darba kopijas tiks saglabātas un kas notiks ar datiem pēc šī termiņa. Tas palīdz izvairīties no situācijas, kur dati tiek saglabāta arī pēc tam, kad to izmantošana vairs nav vajadzīga. Kā viens no veidiem ir tehnoloģiski noteikt automātisku piekļuves tiesību noņemšanu un datu dzēšanu vai arhivēšanu, tādējādi samazinot cilvēcisko termiņu izsekošanas risku.

Tabula 4 – Datu glabāšanas pieejas izvēle

Tehnoloģiskā pieeja	Tipiskie risinājumi	Nosacījumi, kas jāievēro pārvaldot 2. Līmeņa datus	Nosacījumi, kas jāievēro pārvaldot 3. līmeņa datus	Nosacījumi, kas jāievēro pārvaldot 4. līmeņa datus
Lokāla glabāšana uz institucionāli pārvaldītas darbstacijas	Institūcijas izsniegts klēpjdators, vai darba stacija	Pieļaujama tikai kā vide darba kopijām, nevis projekta galvenā glabāšanas vieta.	Pieļaujams izņēmuma gadījumos tikai kā vide darba kopijām, ja darba stacija nostiprināta un tiek ievērotas drošības prasības.	Neizmantot kā datu glabāšanas risinājumu - izmantojams tikai tad, ja darbstacija atbilst droša apstrādes vides nosacījumiem.
Institucionāli pārvaldīta mākoņkrātuve	Institucionāli pārvaldītas koplietojamas dokumentu un failu vides, tostarp SharePoint, OneDrive, Nextcloud, ownCloud.	Ieteicams, kā tipiski piemērotais risinājums projekta datu uzglabāšanai.	Pieļaujams, ja tiek ievēroti datu glabāšanas pamatprincipi un kontrolēta datu drošība.	Neizmantot kā datu glabāšanas risinājumu - izmantojams tikai tad, ja risinājums faktiski darbojas kā kā daļa no kontrolētas droša apstrādes vides, nevis parasta failu krātuve.
Institucionāli pārvaldīta serveru un tīkla glabāšanas infrastruktūra	Universitātes tīkla diski, failu serveri, institucionāli pārvaldīti serveru klasteri.	Ieteicams kā labs standarta risinājums, ja piekļuve un infrastruktūra tiek pārvaldīta centralizēti.	Ieteicams kā labs standarta risinājums, ja piekļuve un infrastruktūra tiek pārvaldīta centralizēti.	Pieļaujams, ja risinājums faktiski darbojas kā daļa no kontrolētas droša apstrādes vide.
Izvērtēti un saskaņoti ārējie mākoņpakalpojumi	Ārējie mākoņpakalpojumi, kas nav institūcijas pamatrisinājumi, piemēram, B2Safe, Azure Blob storage, AWS S3, GCP Cloud Storage	Pieļaujams, ja risinājums ir iepriekš izvērtēts un apstiprināts un atbilst datu uzglabāšanas prasībām (datu rezidence, pakalpojuma sertifikācija u.tml.).	Pieļaujams, ja risinājums ir iepriekš izvērtēts un apstiprināts un atbilst datu uzglabāšanas prasībām (datu rezidence, pakalpojuma sertifikācija u.tml.).	Neizmantot, izņemot īpaši apstiprinātus gadījumus, kur tas ir pielīdzināms kontrolētai drošas apstrādes videi
Fiziski datu nesēji	USB zibatmiņa, ārējais disks.	Nav ieteicams, izmantojami tikai izņēmuma gadījumos īslaicīgai glabāšanai vai pārnešanai.	Neizmantot kā datu glabāšanas risinājumu	Neizmantot kā datu glabāšanas risinājumu
Personīgie glabāšanas risinājumu konti	Personīgais e-pasts, personīgais OneDrive/Google Drive/Dropbox konts.	Neizmantot kā datu glabāšanas risinājumu	Neizmantot kā datu glabāšanas risinājumu	Neizmantot kā datu glabāšanas risinājumu

Tehnoloģiskā pieeja	Tipiskie risinājumi	Nosacījumi, kas jāievēro pārvaldot 2. Līmeņa datus	Nosacījumi, kas jāievēro pārvaldot 3. līmeņa datus	Nosacījumi, kas jāievēro pārvaldot 4. līmeņa datus
Drošas apstrādes vide	Skatīt sadaļu 4	Ieteicams, kā visdrošākais risinājums	Ieteicams, kā visdrošākais risinājums	Ieteicams, kā visdrošākais risinājums

Ieteicamā pieeja šī līmeņa datu apstrādei.

Pieļaujams ar nosacījumiem - nepieciešams izvērtējums un atbilstoši kontroles pasākumi.

Neizmantot šī līmeņa datiem. Atsevišķos gadījumos pieļaujams, piemēram, drošas apstrādes vides ietvaros.

3.2.1 Datu kopīgošana pētniecības procesā

Datu kopīgošana pētniecības laikā ir jāorganizē tā, lai iesaistītajām personām būtu pieejami tikai tie dati, kas nepieciešami konkrēta pētniecības uzdevuma izpildei, vienlaikus saglabājot kontroli pār piekļuvi, datu kopiju veidošanos, versijām, eksportu un datu izmantošanas vidi. Praktiski tas nozīmē, ka datu kopīgošana nav uzskatāma par atsevišķu tehnisku darbību, bet gan par glabāšanas un apstrādes procesa turpinājumu.

Līdzīgi kā citos datu apstrādes posmos, ievērojot pamatprincipus datu kopīgošanai pētniecības laikā, tiek paaugstināts datu drošības līmenis:

- Datus ieteicams kopīgot tajā pašā vidē, kur tie tiek glabāti vai apstrādāti, nevis veidojot papildu kopijas citās platformās vai nosūtot tos pa atsevišķiem kanāliem.
- Ieteicams kopīgot tikai to datu apjomu un detalizācijas pakāpi, kas nepieciešama konkrētajam sadarbības uzdevumam, nevis visu datu kopu pēc noklusējuma. Tas palīdz mazināt risku, ka plašāks lietotāju loks iegūst piekļuvi datiem, kas tiem nav vajadzīgi.
- Kopīgojot datus, piekļuve piešķirama tikai konkrētām personām vai skaidri definētām grupām, nevis izmantot plašas vai grūti pārskatāmas piekļuves tiesības. Tas ir īpaši svarīgi projektos, kuros iesaistīti vairāki partneri ar dažādām lomām pētniecības procesā.
- Piekļuve kopīgotajiem datiem jāpiešķir uz ierobežotu un pārskatāmu laiku.
- Jānodrošina iespēja pārskatīt, kurš lietotājs, kad un kādā apjomā piekļuvis kopīgotajiem datiem.
- Jānodrošina iespēja kontrolēt datu lejupielādi, automātiski sinhronizāciju uz ierīcēm un iznešanu no pārvaldītās vides, gadījumā, ja to pieprasa attiecīgais drošības līmenis.

Turklāt datu kopīgošanas laikā jāņem vērā piešķirtais datu aizsardzības līmenis. Tas ietekmēs kādas kontroles un tehniskie risinājumi ir piemērojami, lai nodrošinātu piemēroto datu drošības līmeni.

Ja dati pētniecības laikā tiek glabāti datu devēja infrastruktūrā nevis institūcijas infrastruktūrā, uz tiem joprojām attiecas tie paši tehniskie un drošības principi. Papildu pirms šo datu kopīgošanas ar citiem pētniekiem ir jāsaņem attiecīgā datu devēja piekrišana. Praktiski tas nozīmē, ka datu devējs šajā procesā lemj, vai tiek atļauta datu kopīgošanu ar papildu pētniekiem.

Tabula 5 – Datu kopīgošanas pamatprincipi atbilstoši datu aizsardzības līmenim

Datu aizsardzības līmenis	Ieteicamā kopīgošanas pieeja	Minimālie nosacījumi	Papildu prasības un ierobežojumi
2. līmeņa dati	Dati var tikt kopīgoti institucionāli pārvaldītā sadarbības vidē, piemēram, projekta darba vidē, dokumentu sadarbības vidē vai koplietojamā failu krātuvē, ja vide ļauj piešķirt piekļuvi konkrētiem lietotājiem vai grupām	Piekļuve jāpiešķir tikai identificētiem lietotājiem. Publiskas saites nav pieļaujamas. Jānodrošina vismaz pamata piekļuves kontrole un iespēja pārskatīt, kam dati ir pieejami	Dati nedrīkst tikt kopīgoti plašāk, nekā nepieciešams konkrētā projekta darbam. Vēlams nodrošināt izmaiņu un piekļuves izsekojamību.
3. līmeņa dati	Dati kopīgojami tikai ierobežotam lietotāju lokam pārvaldītā vidē ar	Piekļuve jāierobežo šaurām lietotāju grupām. Attālinātai vai ārējai	Ja kopīgošanā iesaistīti ārēji partneri, ieteicamā pieeja ir darbs vienotā

Datu aizsardzības līmenis	Ieteicamā kopīgošanas pieeja	Minimālie nosacījumi	Papildu prasības un ierobežojumi
	pastiprinātu piekļuves kontroli. Priekšroka dodama kopīgam darbam vienotā institucionāli pārvaldītā risinājumā, nevis datu kopiju izplatīšanai starp iesaistītajām pusēm.	piekļuvei jāparedz MFA. Jāizvērtē, vai nav jāierobežo datņu lejupielāde, automātiska failu sinhronizācija uz ierīcēm un citi nekontrolētas kopēšanas ceļi	pārvaldītā vidē vai piekļuve kontrolētam resursam ar papildu drošības slāņiem. VPN var būt viens no papildu kontroles mehānismiem, bet nav uzskatāms par pietiekamu aizsardzību pats par sevi.
4. līmeņa dati	Dati kopīgojami tikai īpaši kontrolētā vidē, kas faktiski darbojas kā droša apstrādes vide. Par noklusējuma pieeju jāuzskata kontrolēta piekļuve vienotai darba videi, nevis datu kopiju nosūtīšana vai lokāla glabāšana pie lietotājiem.	Jāspēj ierobežot vai pārvaldīt datu pievienošanu, lejupielādi, kopēšanu, eksportu un citas datu iznešanas iespējas; jānodrošina pastiprināta auditējamība un pārskatāms piekļuves režīms	Ja ar datiem strādā vairāki pētnieki, tiem jānodrošina piekļuve vienai un tai pašai kontrolētai videi, lai samazinātu nepieciešamību pēc datu pārvietošanas starp personām, ierīcēm vai organizācijām.

Tabula 6 – Datu kopīgošanas pieejas izvēle

Tehnoloģiskā pieeja	2. Līmeņa datu kopīgošana	3. Līmeņa datu kopīgošana	4. Līmeņa datu kopīgošana
Lokāla glabāšana uz institucionāli pārvaldītas darbstacijas	Nav ieteicams, jo nav piemērots vairāku lietotāju kopdarbam un palielina lokālu kopiju veidošanās risku.	Neizmantot kopīgošanai	Neizmantot kopīgošanai
Institucionāli pārvaldīta mākoņkrātuve	Ieteicams, ja piekļuve tiek piešķirta konkrētiem lietotājiem vai grupām un netiek izmantotas publiskas saites.	Ieteicams, ja piekļuve tiek piešķirta konkrētiem lietotājiem vai grupām un netiek izmantotas publiskas saites.	Nav ieteicams, ja vien risinājums faktiski nenodrošina kontrolētu vidi ar stingri ierobežotu datu iznešanu.
Institucionāli pārvaldīta serveru un tīkla glabāšanas infrastruktūra	Ieteicams, organizējot piekļuvi infrastruktūrai centralizēti un tikai iesaistītajām personām.	Ieteicams, organizējot piekļuvi infrastruktūrai centralizēti un tikai iesaistītajām personām.	Ieteicams tikai tad, ja kopīgošana notiek kontrolētā apstrādes vidē un dati nav brīvi eksportējami uz gala iekārtām.
Izvērtēti un saskaņoti ārējie mākoņpakalpojumi	Ieteicams, ja risinājums ir iepriekš izvērtēts un nodrošina nepieciešamās drošības prasības, piekļuve tiek piešķirta konkrētiem lietotājiem vai grupām un netiek izmantotas publiskas saites.	Ieteicams, ja risinājums ir iepriekš izvērtēts un nodrošina nepieciešamās drošības prasības, piekļuve tiek piešķirta konkrētiem lietotājiem vai grupām un netiek izmantotas publiskas saites.	Neizmantot, izņemot gadījumus, kad pakalpojums faktiski darbojas kā apstiprināta droša apstrādes vide.
Fiziski datu nesēji	Nav ieteicams, kopīgošana iespējama tikai nododot datu nesēju, neefektīvs risinājums, jo neatļauj vairākām personām vienlaicīgi strādāt ar datiem. Izņēmuma gadījumos iespējama datu kopēšana uz vairākiem datu nesējiem.	Neizmantot kopīgošanai	Neizmantot kopīgošanai
Personīgie glabāšanas risinājumu konti	Neizmantot kopīgošanai	Neizmantot kopīgošanai	Neizmantot kopīgošanai
Drošas apstrādes vide (skatīt sadaļu 4)	Ieteicams, kā visdrošākais risinājums	Ieteicams, kā visdrošākais risinājums	Ieteicams, kā visdrošākais risinājums

Ieteicamā pieeja šī līmeņa datu apstrādei.
Pieļaujams ar nosacījumiem - nepieciešams izvērtējums un atbilstoši kontroles pasākumi.
Neizmantot šī līmeņa datiem. Atsevišķos gadījumos pieļaujams, piemēram, drošas apstrādes vides ietvaros.

3.3 Datu apstrāde un analīze

Datu apstrādes un analīzes posmā aizsargājamu datu pārvaldības risks parasti ir augstāks nekā glabāšanas vai nodošanas posmā, jo šajā brīdī dati tiek tīrīti, strukturēti, sasaistīti ar citām datu kopām, analizēti un izmantoti rezultātu iegūšanai. Tāpēc šajā posmā būtiski ir ne tikai tas, kādi rīki tiek izmantoti, bet galvenokārt tas, kādā vidē šie rīki tiek izmantoti, kam ir piekļuve datiem un cik lielā mērā iespējams kontrolēt datu kustību un rezultātu iznešanu.

Datu apstrāde pētniecībā var notikt, izmantojot ļoti dažādus risinājumus un programmatūru, kā rezultātā konkrētas programmatūras izmantošana ir vērtējuma konkrētas apstrādes vajadzībām. Šīs sadaļas mērķis nav mēģināt definēt visu atļauto programmatūru sarakstu. Praktiski viens no svarīgākajiem nosacījumiem ir nevis konkrētais risinājums, bet tas, lai datu apstrāde notiktu institucionāli nodrošinātā, institucionāli apstiprinātā vai citādi kontrolētā vidē, kas ir piemērota konkrētajam datu aizsardzības līmenim.

Pamatprincipi, kas attiecināmi uz visiem datu aizsardzības līmeņiem datu apstrādes posmā.

- **Priekšroka dodama institucionāli nodrošinātiem vai institucionāli apstiprinātiem apstrādes risinājumiem.** Ja tiek izmantots ārējs vai specializēts risinājums, ieteicams to iepriekš izvērtēt un saskaņot, kā arī izvērtēt tā lietošanu nostiprinātā darba vidē.
- **Aizsargājamu datu apstrādei nevajadzētu izmantot publiskus vai neizvērtētus rīkus, kas var radīt nekontrolētu datu nodošanu vai sekundāru apstrādi.** Tas attiecas arī uz gadījumiem, kad rīks ir ērts vai plaši izmantots, bet nav skaidrs, kur dati tiek apstrādāti, vai tie tiek saglabāti ārpus institūcijas kontroles, vai tie var tikt izmantoti pakalpojuma sniedzēja vajadzībām.
- **Datu apstrādes laikā ieteicams pēc iespējas samazināt datu pārvietošanu starp vairākām vidēm.** Ja vien tas nav pamatoti nepieciešams, dati nebūtu jākopē no glabāšanas vides uz atsevišķu lokālu vidi, pēc tam uz citu apstrādes vidi un vēlāk atpakaļ. Jo vairāk pārvietošanas un starpkopiju, jo mazāk pārskatāma kļūst datu aprite un jo grūtāk ir nodrošināt kontroli pār piekļuvi, versijām un dzēšanu.
- **Ja analīzes laikā nepieciešams pievienot papildu programmatūru, tas jādara tikai kontrolētā un iepriekš izvērtētā kārtībā.** Pirms jauna rīka izmantošanas ir atkārtoti jāveic tehnoloģiskā izvērtēšana, lai nepieļautu, ka paplašinoties analīzes vajadzībām netiek ievērota drošības prakse.
- **Ja apstrādes laikā dati tiek sasaistīti ar citām datu kopām, būtiski pārveidoti vai izmantoti tā, ka var pieaugt identificēšanas, izpaušanas vai citas neatļautas izmantošanas risks, apstrādes pieeja jāizvērtē atkārtoti.** Tas attiecas arī uz gadījumiem, kad apstrādes rezultātā rodas atvasināti dati, modeļi vai citas jaunas datu vienības, kuru aizsardzības līmenis var atšķirties no sākotnēji izmantotajiem datiem
- **3. un 4. līmeņa datu apstrādei jābūt iespējai ierobežot datu lejupielādi, kopēšanu un citu iznešanu no apstrādes vides.** Jo īpaši 4. līmeņa datiem apstrādei parasti jānotiek drošā apstrādes vidē vai citā līdzvērtīgi kontrolētā vidē. No analīzes vides iznesami tikai tie rezultāti vai starprezultāti, kuru iznešana ir pamatota un atbilst piemērojamajam datu aizsardzības līmenim un datu izmantošanas nosacījumiem.

Datu apstrāde ar mākslīgā intelekta rīkiem

Mākslīgā intelekta, jeb MI, rīku izmantošana šī dokumenta kontekstā nav uzskatāma par atsevišķu datu apstrādes kategoriju, bet gan par vienu no iespējamiem datu apstrādes un analītikas rīkiem, uz kuru attiecas tie paši pamatprincipi un prasības kā uz jebkuru citu datu apstrādes programmatūru vai ārēju pakalpojumu.

MI rīki var būt noderīgs atbalsts pētniecībā, taču tie nemaina pamatprincipus, kas jāievēro datu aizsardzībai apstrādes posmā. Katrs MI izmantošanas gadījums jāvērtē kā potenciāla datu nodošana apstrādei, kas pakļauta papildu riskiem.

Mākslīgā intelekta, jeb MI, rīki arvien biežāk tiek izmantoti pētniecībā, piemēram, datu analīzei, koda ģenerēšanai, teksta sagatavošanai vai citiem nolūkiem.

Vienlaikus MI rīku izmantošana var radīt papildu riskus, jo šādi rīki nereti darbojas kā ārēji pakalpojumi ar ierobežotu pārskatāmību, un to ģenerētie rezultāti var būt neprecīzi, nepilnīgi vai neatbilstoši konkrētajam pētniecības kontekstam. Tādēļ katrs MI rīka izmantošanas gadījums ir izvērtējams atsevišķi, ņemot vērā paredzēto lietojumu, apstrādājamo datu raksturu un iespējamos riskus. Konkrētā MI rīka – produkta vai modeļa izmantošana, vērtējama kontekstā ar tehnoloģisko pieeju, kas tiks izmantota tā darbināšanai.

Jāņem vērā, ka MI funkcionalitāte var būt iebūvēta arī ikdienā izmantotās lietotnēs un platformās. Šādos gadījumos datu nodošana MI apstrādei var notikt nepastarpināti vai lietotājam ne vienmēr pilnībā apzināmā veidā, tādēļ pirms jebkādu tehnoloģisko risinājumu izmantošanas ir jāizvērtē, vai konkrētais rīks neiekļauj šādu funkcionalitāti.

Zemāk sniegti daži piemēri, kas ilustrē, kā MI rīki var tikt pielietoti dažādos pētniecības projekta posmos un kādi aspekti ir jāizvērtē, lai nodrošinātu, ka aizsargāti dati netiek nesankcionēti izpausti. Piemēri nav izsmeļoši, jo katrs MI izmantošanas gadījums jāvērtē individuāli atbilstoši pētniecības mērķim, datu aizsardzības līmenim un piemērojamajiem institūcijas vai datu devēja ierobežojumiem.

Tabula 7 – Praktiski sastopamie MI rīku izmantošanas scenāriji

Izmantotais MI rīks	Situācija	Izmantošanas vērtējums	Galvenie apsvērumi	Drošāka pieeja
Iebūvēta MI funkcionalitāte sanāksmju platformās (piem., MS Teams)	Pētnieks izmanto sanāksmju platformu sanāksmju organizēšanai un iespējo, piemēram, automātisku transkriptu sagatavošanu.	Pieļaujams ar nosacījumiem. Jāizvērtē sadarbībā ar IT atbalstu, vai MI funkcionalitātes izmantošanas laikā dati netiek nodoti ārējam pakalpojuma sniedzējam.	Jānoskaidro, kā konkrētā programmatūras licence apstrādā datus, kur dati tiek glabāti un nodoti apstrādei, vai tie tiek izmantoti pakalpojuma uzlabošanai.	Pirms izmantošanas ar aizsargājamiem datiem konsultēties ar IT atbalstu. Organizējot sensitīvākas sarunas atturēties no MI izmantošanas.
MI izmantošana programmēšanas un tehniskam atbalstam	Pētnieks izmanto MI rīku, lai sagatavotu R/Python kodu, pārbaudītu kļūdu skriptā vai saņemtu skaidrojumu par datu analīzes metodi.	Pieļaujams, ja MI rīkā netiek ievadīti aizsargājami dati vai konfidenciāls projekta saturs.	Jāpārliecinās, ka kodā, kļūdu paziņojumos, repozitorijos vai kopīgotajos failos nav personas datu, sensitīvu mainīgo, API atslēgu, paroļu, datubāzu savienojumu vai komerciāli	Izmantot sintētiskus datus, vienkāršotus mainīgo nosaukumus un vispārīgus piemērus. Pirms koda vai repozitorija kopīgošanas veikt papildu pārbaudi, lai tajā nebūtu

Izmantotais MI rīks	Situācija	Izmantošanas vērtējums	Galvenie apsvērumi	Drošāka pieeja
			konfidenciālas informācijas.	aizsargājamas informācijas.
MI modeļa apmācība vai pielāgošana ar aizsargājamiem datiem	Projektā tiek izmantoti, piemēram, veselības dati, citi 4. līmeņa dati, MI modeļa apmācībai vai pielāgošanai.	Augsta riska scenārijs, kas pieļaujams tikai kontrolētā vidē. Šādam gadījumam jāpiemēro drošas apstrādes vides prasības. (Skatīt 4. nodaļu)	Apmācības dati, modeļa faili, izvades rezultāti var saturēt vai netieši atklāt aizsargājamu informāciju. Arī pats apmācītais modelis var kļūt par aizsargājamu datu vienību/ elementu.	Izmantot drošu apstrādes vidi vai līdzvērtīgi kontrolētu vidi. (Skatīt 4. nodaļu) Pirms modeļa, tā rezultātu vai failu iznešanas jāveic atsevišķs risku izvērtējums.
MI ģenerēta kopsavilkuma vai rezultātu izmantošana publikācijā	Pētnieks izmanto MI, lai sagatavotu pētījuma rezultātu kopsavilkumu, tabulas saturu vai publikācijas tekstu.	Ja MI rīkā tiek ievadīti aizsargājami dati tie var tikt nodoti ārējam pakalpojuma sniedzējam vai apstrādāti ārpus institūcijas kontrolētās vides. Arī tad, ja MI rīks ir institucionāli apstiprināts, MI ģenerētais rezultāts var netīši atklāt pārāk detalizētus rezultātus kas vēl nav sagatavoti publicēšanai.	Datu nodošanas risks: aizsargājami dati var tikt nodoti ārējam apstrādātājam. Izvades risks: arī apstiprināts rīks var ģenerēt tekstu, kas atklāj pārāk detalizētu vai vēl nepublicējamu informāciju.	MI rīkā ievadīt tikai tādu informāciju, kuru drīkst apstrādāt attiecīgajā rīkā. Publikācijā izmantot tikai pārbaudītus, anonimizētus, agregētus un publicēšanai saskaņotus rezultātus.

Tabula 8 – Datu apstrādes pieejas izvēle

Tehnoloģiskā pieeja	Tipiskie risinājumi	Nosacījumi, kas jāievēro pārvaldot 2. līmeņa datus	Nosacījumi, kas jāievēro pārvaldot 3. līmeņa datus	Nosacījumi, kas jāievēro pārvaldot 4. līmeņa datus
Izvērtēti un saskaņoti mākoņpakalpojumi	Ārējie mākoņpakalpojumi, kas nav organizācijas pamatrisinājumi, piemēram, AWS (Lambda/ AppRunner / AWS EC2, Bedrock), Azure (Functions/ Container Apps/ Azure Virtual Machines / Microsoft Foundry), GCP (Cloud functions/ Cloud Run/ Compute Engine / Vertex AI)	Ieteicams tikai ar nosacījumiem. Drīkst izmantot tikai tad, ja pakalpojums ir iepriekš izvērtēts, ir skaidra datu rezidence, piekļuve ir ierobežota un pakalpojuma drošības nosacījumi ir pārskatīti.	Ieteicams tikai ar nosacījumiem. Nepieciešama iepriekšēja saskaņošana. Jābūt pārliecībai, ka vide nodrošina ierobežotu piekļuvi, auditējamību un nekontrolētas datu kopēšanas vai koplietošanas ierobežošanu.	Pieļaujami tikai tad, ja mākoņvide faktiski darbojas kā droša apstrādes vide vai cita līdzvērtīgi kontrolēta apstrādes vide.
Universitātes resursi	Koplietota universitātes infrastruktūra (serveri), universitātes nodrošināta apstrādes programmatūras vide (R / Python / SPSS / MI modeļi vai aplikācijas, u.c.), attālināta darbvirsma.	Ieteicams kā pamata izvēle datu apstrādei, jo vide parasti ir institucionāli pārvaldīta, ar kontrolētu piekļuvi, atjauninājumiem, žurnālēšanu un skaidrāku atbildību sadalījumu.	Ieteicams. Īpaši, ja dati tiek apstrādāti universitātes pārvaldītās darba stacijās, serveros vai attālinātās darbvirsmās, kur piekļuve un konfigurācija tiek centralizēti kontrolēta un tiek nodrošināts tehniskais atbalsts.	Ieteicams tikai ar nosacījumiem. Apstrādei jānotiek īpaši kontrolētā universitātes vidē, piemēram, drošā pētniecības vidē vai citā stingri nodalītā apstrādes vidē
Pētnieka pārvaldīti personīgie risinājumi	Personīgs dators, personīgi konfigurētas virtuālās mašīnas, nesaskaņoti ārējie rīki/programmatūra.	Nav ieteicams. Personīgi pārvaldītās iekārtās un vidēs parasti nav pietiekami pārvaldīta un nav piemērota aizsargājamu datu drošai apstrādei.	Neizmantot. Šajā līmenī pētniekam patstāvīgi pārvaldot risinājumu, bez pietiekamām tehniskajām zināšanām, rodas nesamērīgs risks attiecībā uz nesankcionētu piekļuvi datiem	Neizmantot. īpaši aizsargājamu datu apstrāde personīgā datorā vai citā personīgi uzturētā vidē nav pieļaujama.
Zinātniskai darbībai pielāgotas	RTU HPC, EOSC EU Node, EOSC-ENTRUST u.c.	Ieteicams tikai ar nosacījumiem, ja platforma ir izvērtēta	Ieteicams tikai ar nosacījumiem, ja platforma ir izvērtēta	Ieteicams tikai ar nosacījumu, ka platforma nodrošina drošības

Tehnoloģiskā pieeja	Tipiskie risinājumi	Nosacījumi, kas jāievēro pārvaldot 2. līmeņa datus	Nosacījumi, kas jāievēro pārvaldot 3. līmeņa datus	Nosacījumi, kas jāievēro pārvaldot 4. līmeņa datus
mākoņpakalpojumu platformas		pētniecības vajadzībām, nodrošina piekļuves kontroli, projektu nodalīšanu un skaidrus lietošanas noteikumus.	pētniecības vajadzībām, nodrošina piekļuves kontroli, projektu nodalīšanu un skaidrus lietošanas noteikumus.	līmeni, kas ir līdzvērtīgs īpaši kontrolētai drošas apstrādes videi, un tas ir iepriekš izvērtēts un apstiprināts projektam.
Drošas apstrādes vide	Skatīt sadaļu 4	Ieteicams, kā visdrošākais risinājums	Ieteicams, kā visdrošākais risinājums	Ieteicams, kā visdrošākais risinājums

Ieteicamā pieeja šī līmeņa datu apstrādei.
Pieļaujams ar nosacījumiem - nepieciešams izvērtējums un atbilstoši kontroles pasākumi.
Neizmantot šī līmeņa datiem. Atsevišķos gadījumos pieļaujams, piemēram, drošas apstrādes vides ietvaros.

3.4 Datu publicēšana

Datu publicēšana ir viens no noslēdzošajiem pētniecības procesa posmiem, kurā pētījuma dati un datu kopas tiek sagatavotas ilgtermiņa glabāšanai, publicēšanai vai pieejamības nodrošināšanai. Lai gan sākotnēji var šķist, ka tas ir salīdzinoši vienkāršs solis pēc galveno pētniecības darbu pabeigšanas, praksē tam ir jāpievērš būtiska uzmanība. Kvalitatīva datu publicēšana prasa skaidru plānu un strukturētu pieeju, nosakot, kā, kur un ar kādiem piekļuves nosacījumiem dati tiks publicēti vai nodoti glabāšanai.

Publicēšanas iespējas jāvērtē ne tikai pēc sākotnējās datu kopas aizsardzības līmeņa, bet arī pēc konkrētā publicējamā objekta satura un izpaušanas riska. Pētniecības laikā izmantotie aizsargājamie dati var nebūt publicējami pilnā apjomā, taču no tiem iegūtie rezultāti, agregētas tabulas, pseudonimizēti izvaddati, metadatu ieraksti, metodoloģijas apraksti vai citi atvasināti materiāli var būt publicējami, ja tie vairs neatklāj aizsargājamu informāciju un atbilst datu devēja, līgumiskajiem un normatīvajiem nosacījumiem.

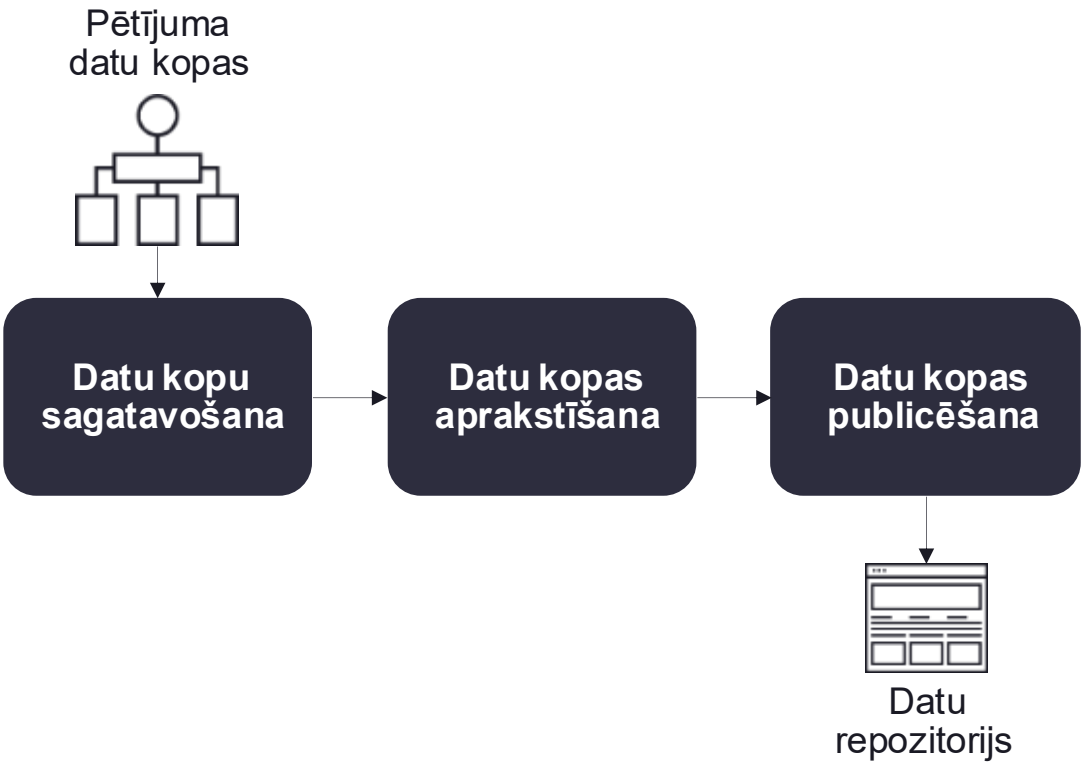
Īpaša piesardzība nepieciešama gadījumos, kad pētījumā izmantoti 3. vai 4. līmeņa dati. Šādos gadījumos pirms publicēšanas jāizvērtē, vai publicējamais materiāls pats par sevi nerada atkārtotas identificēšanas, konfidenciālas informācijas izpaušanas, komerciālu interešu aizskāruma vai citu aizsargātas informācijas izpaušanas risku. Tas attiecas ne tikai uz datu kopām, bet arī uz tabulām, grafikiem, metadatiem un cita veida materiāliem, ja tie ir pārāk detalizēti, balstīti uz mazu novērojumu skaitu vai ļauj sasaistīt rezultātus ar konkrētām personām, organizācijām vai citiem aizsargājamiem objektiem. Praktiski piemēri, kā tas var tikt realizēts:

- Interviju ieraksti un transkripti ar sensitīvu saturu saglabā attiecīgo aizsardzības līmeni un parasti nav publicējami pilnā apjomā. Tomēr anonimizēts tematisks kopsavilkums, citātu fragments bez identificējošām pazīmēm vai secinājumu pārskats var būt publicējams, ja ir izvērtēts un mazināts atkārtotas identificēšanas risks.
- Veselības mikrodati, piemēram, individuāla līmeņa ieraksti par diagnozēm, ārstēšanu vai pacienta pazīmēm, saglabā 4. aizsardzības līmeni. Vienlaikus no tiem iegūta agregēta tabula var būt publicējama, ja tā nesatur retas kombinācijas vai citus elementus, kas ļautu netieši identificēt personas.
- Individuāla līmeņa aptaujas dati ar respondentu vecumu, amatu, darba vietu un brīva teksta atbildēm saglabā attiecīgo aizsardzības līmeni, jo personas var būt tieši vai netieši identificējamas. Tomēr agregēts rezultātu kopsavilkums pa plašākām respondentu grupām vai anonimizēti citāti bez identificējošām pazīmēm var būt publicējami, ja ir mazināts atkārtotas identificēšanas risks.

Datu publicēšanas procesa organizēšana

Datu publicēšana ne vienmēr nozīmē to tūlītēju publisku pieejamību. Dati var tikt publicēti arī ar kontrolētu piekļuvi, piemēram, piešķirot piekļuves tiesības tikai noteiktam lietotāju lokam vai nodrošinot pieeju pēc atsevišķa pieprasījuma. Tāpēc publicēšanas brīdī būtiski ir izvērtēt ne tikai tehnisko publicēšanas risinājumu, bet arī datu pieejamības modeli.

Pirms datu publicēšanas ir jānodrošina, ka saņemtas visas nepieciešamās atļaujas un nepastāv juridiski, līgumiski vai citi ierobežojumi, kas varētu liegt vai ierobežot datu publiskošanu. Īpaša uzmanība jāpievērš tam, vai dati satur komerciāli sensitīvu, konfidenciālu vai citu aizsargājamu informāciju, tostarp personas datus. Vienlaikus ir skaidri jānosaka, kurš kontrolē datus un kurš ir atbildīgs par lēmuma pieņemšanu attiecībā uz to publicēšanu.



Attēls 3 – Datu publicēšanas process

Pirms datu publicēšanas tos ir nepieciešams sagatavot, lai publicētais materiāls būtu saprotams, izmantojams un neradītu nepamatotus riskus. Sagatavošana ietver darbības kā datu kvalitātes pārbaudi, datņu strukturēšanu, lieku vai kļūdainu elementu izņemšanu, versiju sakārtošanu un datu dokumentēšanu. Ja pilnas datu kopas publicēšana nav nepieciešama, jāapsver iespēja publicēt tikai to datu daļu, kas ir būtiska rezultātu pārbaudei, atkārtotai izmantošanai vai metodoloģijas izpratnei. Datu sagatavošanas laikā arī jāizvērtē, vai nepieciešama anonimizācija, pseidonimizācija, agregēšana vai citi aizsardzības pasākumi, īpaši gadījumos, kad dati var iekļaut aizsargājamu informāciju.

Lai publicētie dati būtu atrodami un atkārtoti izmantojami, tiem jābūt pietiekami dokumentētiem un jāpievieno metadati. Tas nozīmē, ka skaidri jāapraksta datu saturs, struktūra, izcelsme, izveides metode, laika ietvars, izmantotās vienības, datu kvalitātes īpatnības, iespējamie ierobežojumi un citi izmantošanai nozīmīgi aspekti. Ja pašus datus nevar publicēt, labā prakse ir publicēt vismaz metadatus, jo tas ļauj citām personām identificēt datu esamību un, ja nepieciešams, vērsties pie datu autora pēc piekļuves vai papildu informācijas.

Datu publicēšanai jāizvēlas uzticams un pārvaldāms repozitorijs vai cita institūcijas saskaņota publicēšanas vide, kas atbilst konkrētajam datu veidam un aizsardzības prasībām. Galvenā priekšroka tiek dota institucionāli pārvaldītiem vai atbalstītiem repozitorijiem. Izvēloties repozitoriju, jāņem vērā ne tikai tehniskā ērtība, bet arī repozitorija uzticamība, ilgtspēja, atbilstība FAIR principiem, un iespēja kontrolēt nepieciešamo piekļuves režīmu. Veicot datu nodošanu uz repozitoriju, jāievēro tie paši drošības principi, kas aprakstīti datu nodošanas sadaļā, atbilstoši datu aizsardzības līmenim.

Tabula 9 – Datu publicēšanas pieejas

Publicēšanas pieeja	Apraksts	Piemērotie datu veidi	Piekļuves ierobežojumi	Tehnoloģiskie aspekti
Atklāta publicēšana	Tiek publicēta pilna datu kopa kopā ar metadatiem, un tā ir tieši pieejama lejupielādei.	Piemērots atvērtiem (1.līmeņa) datiem.	Piekļuve parasti ir publiska un neprasa individuālu apstiprinājumu.	Galvenā uzmanība jāpievērš tam, lai pirms publicēšanas datos nebūtu palikuši identifikatori, konfidenciāli elementi vai cita nejauši izpaužama informācija.
Publicēšana ar embargo	Datu kopa un metadati tiek noguldīti repozitorijā, bet piekļuve pašiem datiem tiek atvērta tikai vēlāk noteiktā datumā vai pēc konkrēta notikuma.	Piemērota datiem, kurus plānots publicēt vēlāk, bet ne uzreiz, piemēram, kamēr tiek veikts pētījums vai spēkā ir pagaidu līgumisks ierobežojums.	Līdz embargo beigām dati nav publiski pieejami. Atsevišķos gadījumos var nodrošināt ierobežotu piekļuvi īpaši noteiktām personām.	Īpaši svarīgi ir pareizi nokonfigurēt embargo iestatījumus, kontrolēt pagaidu piekļuves mehānismus un novērst nejaušu priekšlaicīgu datu atvēršanu.
Ierobežotas piekļuves publicēšana	Publiski pieejami metadati, savukārt pati datu kopa ir pieejama tikai autentificētiem vai noteiktiem nosacījumiem piekritušiem lietotājiem	Piemērota 2. un 3. līmeņa datiem, kurus nevar publicēt atklāti, bet kurus tomēr iespējams padarīt pieejamus ar aizsargpasākumiem.	Piekļuve parasti prasa reģistrāciju, autentifikāciju vai piekrišanu noteiktiem izmantošanas nosacījumiem.	Svarīgi ir lietotāju identitātes uzskaites mehānismi, piekļuves tiesību pārvaldība, piekļuves uzskaite un repozitorija spēja publiski atrādīt metadatus, vienlaikus droši ierobežojot piekļuvi pašiem failiem.
Kontrolētas piekļuves publicēšana	Metadati ir publiski pieejami, bet piekļuve datu kopai tiek piešķirta tikai pēc formālas izvērtēšanas un apstiprināšanas	Piemērota 2. un 3. līmeņa datiem, kurus nevar publicēt atklāti, bet kurus tomēr iespējams padarīt pieejamus ar aizsargpasākumiem.	Piekļuve tiek dota tikai personām, kuras pieprasījušas piekļuvi datu kopai	Svarīgi ir lietotāju identitātes pārbaudes mehānismi, autentifikācijas drošums, piekļuves tiesību pārvaldība un piekļuves apstiprināšanas darba plūsmas. Jānodrošina iespēja ierobežot piekļuvi uz konkrētu termiņu vai atsaukt

Publicēšanas pieeja	Apraksts	Piemērotie datu veidi	Piekļuves ierobežojumi	Tehnoloģiskie aspekti
				to nepieciešamības gadījumā.
Tikai metadatu publicēšana	Tiek publicēti tikai metadati, datu kopas apraksts, citēšanas informācija un piekļuves nosacījumi, bet pati datu kopa netiek publiski izpausta	Piemērota situācijām, kad pašus datus pilnā apjomā publicēt nedrīkst personas datu, konfidencialitātes, autortiesību, līgumisku ierobežojumu, komerciālas sensitivitātes vai citu iemeslu dēļ.	Dati paliek nepieejami vai pieejami tikai pēc atsevišķa pieprasījuma, vēršoties pie atbildīgās personas, bet informācija par to esamību ir publiski atrodama	Būtiskākais risks ir tas, ka sensitīvu informāciju var netīši atklāt metadatos iekļautā informācija.
Tikai rezultātu publicēšana	Netiek publicēta pati datu kopa, tā vietā tiek publicēti tikai apkopoti rezultāti, statistikas tabulas, apstrādāti izvaddati, metodoloģijas apraksti.	Piemērots datiem, kuri ir pārāk aizsargāti, lai tos publicētu pat ar kontrolētu piekļuvi, bet kuru pētījuma rezultātā radītos rezultātus tomēr var kopīgot.	Pamata datu kopas netiek izpaustas, pieejami kļūst tikai atlasīti un pārbaudīti atvasinātie rezultāti.	Galvenā uzmanība jāvērš izvaddatu kontrolei, jo arī apkopotas tabulas, pārāk detalizēti datu griezumi vai sasaistīti izvades faili var atklāt sensitīvu informāciju.

4. Drošas apstrādes vides izmantošana

Droša apstrādes vide ir kontrolēta tehnoloģiskā vide, kurā pētnieki var piekļūt aizsargājamiem datiem, tos glabāt un analizēt, vienlaikus samazinot risku, ka dati tiek nekontrolēti kopēti, pārvietoti vai iznesti ārpus pārvaldītas vides. Praktiski šāda vide apvieno ne tikai tehniskus drošības mehānismus, bet arī piekļuves pārvaldību, auditējamību, programmatūras kontroli un noteiktu datu ievades un izvades kārtību.

Attēls 4 – Drošas apstrādes vides darbības princips

Drošas apstrādes vides izmantošana ir īpaši ieteicama gadījumos, kad projektā tiek apstrādāti individuāla līmeņa dati, dati ar tiešiem vai netiešiem identifikatoriem, pseidonimizēti personas dati, līgumiski ierobežoti dati vai citi dati, kuru neatļauta izpaušana var radīt kaitējumu datu subjektiem, datu devējiem, projekta partneriem vai institūcijai. Šī dokumenta kontekstā droša apstrādes vide visbiežāk ir nepieciešama 3. un 4. līmeņa datiem, bet atsevišķos gadījumos tā var būt pamatota arī 2. līmeņa datiem, ja to pieprasa datu devējs, līgums vai konkrētā pētniecības situācija.

Atsevišķos gadījumos drošas apstrādes vides izmantošana var būt ne vien ieteicama, bet arī izrietēt no piemērojamā normatīvā regulējuma, kuros ir noteiktas paaugstinātas prasības datu aizsardzībai, konfidencialitātei un kontrolētai piekļuvei. Piemēram, Datu pārvaldības akts (DPA) paredz, ka publiskā sektora iestādēm, kas atļauj aizsargātu datu atkalizmantošanu, jānodrošina tehniski apstākļi, kas saglabā privātumu un konfidencialitāti, savukārt Eiropas veselības datu telpas regula (EVDT) sekundārajai izmantošanai skaidri paredz drošas apstrādes vides izmantošanu kā vienu no galvenajiem aizsardzības mehānismiem.

Tabula 10 – Drošas apstrādes vides izmantošana atbilstoši aizsardzības līmenim

2. līmeņa dati	3. līmeņa dati	4. līmeņa dati
Droša apstrādes vide ir vēlama, bet ne vienmēr obligāta. Iespējama arī cita ar pārvaldīta vide, kas nodrošina iepriekšējās sadaļās definētās drošības prasības	Droša apstrādes vide ir ieteicamā noklusējuma pieeja. Iespējams izmantot līdzvērtīgi stingri kontrolētu vidi, ja veikta tās drošības kritēriju izvērtēšana un atbilstoša konfigurēšana	Droša apstrādes vide ir uzskatāma par noklusējuma prasību

Jāņem vērā, ka konkrēta pieeja kā tiek realizēta drošas apstrādes vide var būt ļoti atšķirīga, sākot no lokāli uzturētas izolētas darbstacijas vai virtuālās mašīnas līdz standartizētākiem mākoņpakalpojumiem. Tādēļ atsevišķu risinājumu izvērtēšanai ir lietderīgi izmantot, piemēram, SATRE arhitektūras principus, kas nosaka kādas prasības videi ir jānodrošina, lai tā varētu tikt uzskatīta par drošu apstrādes vidi. Lai vidi varētu uzskatīt par drošu apstrādes

vidi aizsargājamu datu izmantošanai pētniecībā, tai nepieciešams nodrošināt vismaz šādas prasības:

- **Individuāla, personai piesaistīta piekļuve.** Katram lietotājam ir savs konts un koplietoti konti nav pieļaujami.
- **Daudzfaktoru autentifikācija (MFA).** Piekļuve videi jānodrošina ar pastiprinātu autentifikāciju.
- **Piekļuves ierobežošana tikai autorizētiem lietotājiem.** Piekļuves tiesībām jābalstās uz "nepieciešams zināt" un vismazāko privilēģiju principu.
- **Kontrolēta darba vide.** Piekļuve datiem jāorganizē caur pārvaldītu darba vietu, piemēram, virtuālu darbvirsmu, attālinātu sesiju, pārlūkā pieejamu vidi vai citu līdzvērtīgi kontrolētu risinājumu.
- **Atļauto rīku un programmatūras kontrole.** Jābūt noteiktam un pārvaldītam atļautās programmatūras, bibliotēku un pakalpojumu kopumam.
- **Interneta piekļuves kontrole.** Interneta piekļuve ir jāierobežo vai jābloķē pēc noklusējuma, pieļaujot tikai pamatotus un apstiprinātus izņēmumus.
- **Kontrolēta datu ievade un izvade.** Datu importam un eksportam jānotiek kontrolēti, pēc iespējas ar apstiprināšanas un žurnalēšanas mehānismiem.
- **Lietotāju darbību auditācija.** Jānodrošina piekļuves un galveno darbību uzskaite, lai vajadzības gadījumā varētu identificēt veiktās darbības.
- **Loģiska projektu nodalīšana.** Dažādu projektu dati un resursi jānodala tā, lai nepieļautu nejaušu vai neatļautu datu sajaukšanu.
- **Dzīves cikla pārvaldība.** Pēc projekta noslēguma vide, piekļuves tiesības, datu kopijas un pagaidu resursi ir jāpārskata un, ja nepieciešams, jāslēdz vai jādzēš atbilstoši noteiktajai kārtībai.

Papildus iepriekšminētajam, izvēloties konkrētu risinājumu, jāizvērtē arī datu rezidence, rezerves kopēšana, incidentu pārvaldības iespējas, identitātes integrācija ar institucionālajiem kontiem un iespēja tehniski ierobežot datu iznešanu.

Drošas apstrādes vides var tikt īstenotas vairākos veidos atkarībā no institūcijas kapacitātes, pieejamiem resursiem un projekta specifikas.

- Viens no vienkāršākajiem risinājumiem ir izolēta vai stingri ierobežota darba stacija, kas paredzēta konkrētam pētījumam un nav daļa no ikdienas darba vides. Šāda pieeja var būt piemērota atsevišķiem lokāli organizētiem projektiem. Risinājumi šajā kategorijā praksē var būt dažādi, sākot no speciāli izsniegta klēpjdatora vai darbstacijas līdz izolētam serverim.
- Bieži lietota pieeja ir nostiprinātas virtuālās mašīnas, konteineri vai virtuālās darbvirsmas, kur dati paliek centrāli pārvaldītā infrastruktūrā, bet pētnieks pieslēdzas attālināti. Šāda pieeja arī piedāvā iespēju institūcijām uzturēt savā infrastruktūrā nostiprinātas lietojumprogrammas, piemēram, centralizēti pārvaldītus statistikas vai analīzes rīkus. Šādā gadījumā pētniekam tiek sniegta piekļuve tikai konkrētajam rīkam datu apstrādei drošā vidē.
- Mākoņvidē balstīti pašpārvaldīti drošas apstrādes vides risinājumi var tikt veidoti, izmantojot drošas pētniecības vides ietvarus dažādos mākoņproduktos. Piemēram, *Azure Trusted Research Environment (Azure TRE)* ir pielāgots pētniecības vides veidošanai MS Azure vidē, savukārt *AWS Research and Engineering Studio (AWS RES)* ir vide drošu pētniecības darbvietu nodrošināšanai AWS vidē. Šādi risinājumi visbiežāk piedāvā centralizētu identitātes pārvaldību, izolētas darba telpas, pārvaldītu rīku komplektu un labākas mērogošanas iespējas.

- Federēta drošas pētniecības vide iekļauj drošas apstrādes vides, kurās lietotāji pievienojas esošai platformai un izmanto tajā pieejamos rīkus, resursus un pārvaldības mehānismus. Visbiežāk tas tiek piedāvāts kā maksas pakalpojums un viens no šāda veida populāriem risinājumiem pētniecības jomā ir EOSC EU Node. Turklāt šis veids iekļauj arī paveidu, kas ir organizāciju nodrošinātās drošas apstrādes vides, kā, piemēram, Latvijā CSP drošas apstrādes vide vai Somijā Kapseli.

Izvēloties mākoņa vai federētu drošu apstrādes vidi, ir svarīgi pārliecināties par pakalpojuma sniedzēja uzticamību, drošības pārvaldību, auditējamību, datu rezidences prasību izpildi un iespēju tehniski īstenot nepieciešamos ierobežojumus, piemēram, datu iznešanas kontroli, tīkla izolāciju, piekļuves pārvaldību un atļauto rīku katalogu. Neatkarīgi drošības apliecinājumi, piemēram, ISO/IEC 27001, var būt noderīgs uzticamības indikators, bet tie paši par sevi nenozīmē, ka vide automātiski ir piemērota konkrētajam pētniecības pielietojumam - vienmēr jāvērtē arī konkrētās kontroles un pārvaldības procesu atbilstība. ES un Latvijas kontekstā īpaša uzmanība jāpievērš VDAR, EVDT un datu devēju vai projektu līgumos noteiktajām prasībām, savukārt starptautisku projektu gadījumā var būt piemērojami arī citi nosacījumi, piemēram, HIPAA, ja tas attiecas uz konkrēto sadarbību.

Tabula 11 – Drošas apstrādes vides veidu raksturojums

Drošās apstrādes vides veids	Stiprās puses	Ierobežojumi
Izolēta darba stacija	Vienkārši nodrošināt fizisku un tīkla izolāciju. Piemērots šauram lietotāju lokam un nelieliem, lokāli organizētiem projektiem.	Ierobežota elastība sadarbībai, attālinātam darbam un mērogošanai. Augstāka atkarība no lokālās administrēšanas kvalitātes. Grūtāk centralizēti pārvaldīt vairākus projektus.
Nostiprināta virtuālā mašīna / virtuālā darbvirsma	Centralizēta konfigurāciju pārvaldība, ērtāk nodrošināt auditāciju, rezerves mehānismus un kontrolētu programmatūras katalogu. Piemērota gan risinājumam, kas izmitināts paša infrastruktūrā (angļu val. *on-prem*), gan mākoņvidē.	Nepieciešama atbilstoša infrastruktūra un administratīvā kapacitāte. Lietojamība un veiktspēja ir atkarīga no attālinātās piekļuves risinājuma un infrastruktūras kvalitātes.
Mākoņvidē balstīta pašpārvaldīta drošas apstrādes vide Piemēram, Azure TRE, AWS RES, The Turing Data Safe Haven	Mērogojamība, elastīga resursu piešķiršana, izolētas projektu darba telpas, centralizēta identitātes un rīku pārvaldība. Piemērota specializētai analīzei un lielākai skaitļošanas jaudai.	Jāveic rūpīga izvērtēšana par datu rezidenci, izmaksām, datu iznešanas kontroles iespējām un institūcijas spēju pārvaldīt risinājumu. Ne visi mākoņpakalpojumi paši par sevi ir droša pētniecības vide.
Federēta drošas pētniecības vide Piemēram, EOSC EU Node	Gatavs produkts, kas var tikt licencēts kā pakalpojums. Nodrošina mērogojamu pētniecības vidi ar centralizētu piekļuvi datiem, apstrādes rīkiem un skaitļošanas pakalpojumiem. Atbalsta sadarbību, reproducējamu un FAIR principiem atbilstošu pētniecību.	Piekļuve un resursu apjoms ir atkarīgs no lietotāja statusa un piešķirtajām tiesībām. Vide ir piemērotāka atvērtai un federētai pētniecībai nekā ļoti specifiskām, stingri kontrolētām datu apstrādes vajadzībām. Jārēķinās ar pieejamo apstrādes rīku ierobežojumiem.

Drošās apstrādes vides veids	Stiprās puses	Ierobežojumi
	Integrēta autentifikācija un kopīga lietotāju vide atvieglo resursu izmantošanu dažādās institūcijās.	

Dažkārt datu devēji pētniekiem piekļuvi aizsargātiem datiem piešķir tikai ar nosacījumu, ka analīze notiek datu devēja pārvaldītajā tehnoloģiskajā vidē, nevis pētnieka vai institūcijas infrastruktūrā. Šāda pieeja ļauj datu devējam nodrošināt autorizētu piekļuvi, lietotāju autentifikāciju, darbību uzraudzību un auditu, kā arī ierobežot datu lejupielādi ārpus drošās vides.

Latvijā CSP, pētniecības nolūkiem, nodrošina autorizētu piekļuvi drošai apstrādes videi, lai piekļūtu aizsargātiem datiem. Šajā gadījumā pētnieks strādā attālinātās piekļuves vidē un dati netiek iznesti ārpus tās, ja tas nav īpaši atļauts.
Tādēļ drošas pārvaldītas vides izmantošana bieži vien nav papildu izvēle, bet gan priekšnoteikums, lai saņemtu piekļuvi aizsargātiem vai ierobežotas pieejamības datiem.

Ja institūcija pētniekiem vēl nepiedāvā pilnvērtīgu drošas apstrādes vidi kā standarta pakalpojumu, 3. un 4. līmeņa datu apstrādei nav ieteicams automātiski izvēlēties mazāk kontrolētu risinājumu tikai praktisku ierobežojumu dēļ.

Šādos gadījumos jāizvērtē, vai konkrētajam pētījumam iespējams izmantot kādu no citām aprakstītajām pieejām, piemēram, mākoņvidē balstītu drošas apstrādes vides risinājumu vai federētu drošas pētniecības vidi. Veicot izvērtējumu, būtiski pārbaudīt, vai tas faktiski nodrošina konkrētajam datu aizsardzības līmenim nepieciešamās kontroles. Jāņem vērā arī pakalpojuma lietošanas noteikumi, līgumiskie nosacījumi, datu apstrādes vieta, drošības apliecinājumi vai sertifikācija un tas, vai pakalpojums ir piemērots konkrētajam datu veidam un apstrādes mērķim. (skatīt 4. nodāļā aprakstītos aspektus) Šādu izvērtējumu ieteicams veikt kopā ar institūcijas IT atbalstu, jo risinājuma piemērotība bieži ir atkarīga no tehniskās konfigurācijas un drošības kontroļu praktiskās īstenošanas.

Ārēji vai federēti drošas apstrādes vides pakalpojumi bieži ir maksas pakalpojumi, tādēļ jau projekta plānošanas posmā jāparedz arī to izmaksas, pieejamība un ieviešanas laiks. Ja pārejas risinājums nenodrošina nepieciešamo aizsardzības līmeni, 4. līmeņa datu apstrāde jāatliek vai jāorganizē citā apstiprinātā vidē.

5. Tehnoloģiskā pieeja un pārvaldība

5.1 Minimālās kontroles atbilstoši tehnoloģiskajai pieejai

Šajā sadaļā apkopotas ieteicamās minimālās kontroles tehnoloģiskajām pieejām, kuras var izmantot aizsargājamu datu nodošanai, glabāšanai, kopīgošanai un apstrādei pētniecībā. Sadaļas mērķis ir sniegt atsauces punktu, lai varētu izvērtēt konkrētu tehnoloģisko risinājumu pēc kādām minimālajām drošības un pārvaldības prasībām tam jāatbilst attiecīgajā datu aizsardzības līmenī.

Tabula nav paredzēta kā pilnīgs tehniskais standarts vai detalizēta konfigurācijas instrukcija katram risinājumam, jo katrs konkrētais produkts piedāvā atšķirīgus nosacījums. Tā sniedz praktisku minimālo prasību ietvaru, kuru institūcija var izmantot, izvērtējot, vai konkrētā tehnoloģiskā pieeja ir piemērota 2., 3. vai 4. līmeņa datiem.

Detalizētāku informāciju par prasībām, kas jāievēro, pārvaldot dažāda veida IT risinājumus, iespējams iegūt kiberdrošības jomā publicētajos informatīvajos materiālos un praktiskajās vadlīnijās. Kā piemērus var minēt ENISA izstrādāto Technical Implementation Guidance un Handbook on Security of Personal Data Processing, kuros sniegti strukturēti ieteikumi drošības pasākumu ieviešanai un uzturēšanai informācijas sistēmās.

Minētie materiāli kalpo kā praktisks atbalsts organizācijām, plānojot, ieviešot un uzraugot tehniskos un organizatoriskos drošības risinājumus, kā arī nodrošinot personas datu apstrādes atbilstību piemērojamajām prasībām. Organizācijas kā ENISA regulāri aktualizē šīs vadlīnijas, ņemot vērā kiberdrošības apdraudējumu attīstību, jaunas tehnoloģijas un nozares labāko praksi.

Norādes par konkrētām informācijas sistēmām un programmām jāizvērtē individuāli, ņemot vērā, ka katra no tām tās īsteno atšķirīgi. Izvērtējums jābalsta uz ražotāja dokumentāciju, kā arī uz citiem pieejamiem drošas konfigurācijas un lietošanas avotiem, piemēram, CIS Benchmark List , kurā iekļautas rekomendācijas par programmatūras un tehnoloģisko resursu drošības konfigurāciju.

Tabula 12 – Minimālās tehnoloģiskās kontroles atbilstoši tehnoloģiskajai pieejai

Tehnoloģiskā pieeja	2. līmeņa dati	3. līmeņa dati	4. līmeņa dati
Fiziski datu nesēji	Fiziski datu nesēji izmantojami tikai izņēmuma gadījumos. Dati uz nesējiem obligāti jāšifrē, izmantojot spēcīgus kriptogrāfiskos algoritmus. Piekļuve nesējiem jāaizsargā ar papildu autentifikāciju. Jānodrošina datu nesēju inventarizācija, izsniegšanas un atgriešanas uzskaite.	Netiek ieteikts. Ja izņēmuma gadījumā tiek izmantots jāievēro 2. līmeņa prasības.	Neizmantot

Tehnoloģiskā pieeja	2. līmeņa dati	3. līmeņa dati	4. līmeņa dati
	Pēc glabāšanas pabeigšanas dati droši jādzēš vai nesēji fiziski jāiznīcina.		
Datu apmaiņa starp divām sistēmām	Datu pārsūtīšanai jāizmanto šifrēti transmisijas protokoli, piemēram, TLS aizsargāti savienojumi vai droši tuneļi. Jānodrošina saņēmēja sistēmas pārbaude un jāierobežo piekļuve tikai konkrētiem galapunktiem. Datu nodošanas fakts un kļūdas jāreģistrē žurnālos. Ieteicams nodrošināt pārsūtīto datu integritātes pārbaudi pēc saņemšanas.	Ietver 2. līmeņa prasības un papildus: Datu apmaiņa pieļaujama tikai pa iepriekš apstiprinātiem savienojumiem (piemēram, TLS 1.2. vai 1.3., SFTP, SSH vai VPN tuneļiem). Starpkopijas gala lietotāju iekārtās nav pieļaujamas. Atslēgu vai sertifikātu nodošana jāveic atsevišķā, drošā kanālā.	Ietver 3. līmeņa prasības un papildus: Datu apmaiņa pieļaujama tikai starp izolētām, savstarpēji autentificētām sistēmām, izmantojot minimālu un uzraudzītu savienojumu.
Institucionāli pārvaldītas darbstacijas	Datu apstrāde pieļaujama tikai institucionāli pārvaldītās darba stacijās. Jānodrošina pilna diska šifrēšana, ekrāna automātiska bloķēšana un stingra paroles politika. Administratoru tiesības jānodala no ikdienas lietotāju piekļuves. Jābūt iespējai tehniski kontrolēt ārējo interfeisu izmantošanu. Darba stacijām regulāri jāsaņem drošības atjauninājumi un jābūt iespējai centralizēti ievākt drošības žurnālus.	Ietver 2. līmeņa prasības un papildus: Ārējo datu nesēju izmantošana pēc noklusējuma jāierobežo. (piem, datu kopēšana uz zibatmiņas). Programmatūras instalēšana pieļaujama tikai ar institucionālu apstiprinājumu. Jānodrošina pastiprināta lietotāju darbību žurnalēšana ar žurnālfailu apskatīšanas iespējam centralizēti.	Pieļaujamas tikai kā izolētas drošas apstrādes vides sastāvdaļa, kur darba stacija ir nostiprināta papildu ar kiberdrošības konfigurāciju (datu iznešanas ierobežojumi, šifrēšana, paroles, u.c.) un bez ārējās tīkla piekļuves un neapstiprinātas perifērijas ierīcēm. Jāierobežo citu personu fiziska piekļuve darba stacijai - darba stacija nedrīkst atrasties citām personām brīvi pieejamā lokācijā.

Tehnoloģiskā pieeja	2. līmeņa dati	3. līmeņa dati	4. līmeņa dati
Institucionāli pārvaldīta mākoņkrātuve	Piekļuve datiem jānodrošina tikai pilnvarotiem lietotājiem, ieteicams izmantojot institucionālas identitātes. Ieteicams izmantot papildus drošības elementus autentifikācijai MFA. Publiskas koplietošanas saites jāatspējo pēc noklusējuma. Piekļuvei jānotiek, izmantojot šifrētus savienojumus. Jānodrošina versiju vēsture, datu atjaunošanas iespējas un piekļuves žurnālu saglabāšana.	Papildus 2. līmeņa prasībām: Piekļuvei jābūt ierobežotai ar papildu nosacījumiem piemēram, tikai ar institūcijas kontiem. Izmantot MFA. Pēc noklusējuma jāierobežo sinhronizācija un lejupielādes iespējas. Jāierobežo dalīšanās ar lietotājiem ārpus institūcijas kontiem.	Pieļaujama tikai tad, ja risinājums ir sasaistīts ar kontrolētu apstrādes vidi, skatīt sadaļu 4
Institucionāli pārvaldīta serveru un tīkla glabāšanas infrastruktūra	Piekļuve jānodrošina, izmantojot individuālus kontus un lomu balstītu tiesību pārvaldību. Administratīvā piekļuve jāveic tikai caur šifrētiem protokoliem. Dati loģiski jānodala starp projektiem. Jānodrošina regulāra rezerves kopēšana un atjaunošanas testēšana.	Papildus 2. līmeņa prasībām: Jānodrošina MFA Piekļuve resursiem jāierobežo izmantojot VPN un Zero Trust principus Jāierobežo datu kopēšanas iespējas uz gala iekārtām Jānodrošina pārskatāma un regulāra darbību žurnalēšana un piekļuves uzskaite.	Pieļaujama tikai tad, ja risinājums ir sasaistīts ar kontrolētu apstrādes vidi, skatīt sadaļu 4
Izvērtēti un saskaņoti ārējie mākoņpakalpojumi	Pirms izmantošanas jāveic izvērtējums par: Datu rezidenci atbilstoši normatīvajam regulējumam; Datu izolācija starp projektiem; Piekļuves kontroles mehānismi, kas atbalsta MFA, lietotāju tiesību	Pirms izmantošanas jāveic izvērtējums par: Datu rezidenci atbilstoši normatīvajam regulējumam; Datu izolācija starp projektiem; Piekļuves kontroles mehānismi, kas atbalsta MFA, lietotāju tiesību	Pieļaujama tikai tad, ja risinājums ir sasaistīts ar kontrolētu apstrādes vidi, skatīt sadaļu 4 Pirms izmantošanas jāveic izvērtējums par: Datu rezidenci atbilstoši normatīvajam regulējumam;

Tehnoloģiskā pieeja	2. līmeņa dati	3. līmeņa dati	4. līmeņa dati
	iestatīšanu, auditāciju; Atbilstība normatīvajam datu kopai saistošajam regulējumam (GDPR, EHDS, DPA u.c.); Atzīti kiberdrošības sertifikāti, piem., ISO/IEC 27001	iestatīšanu, auditāciju; Atbilstība normatīvajam datu kopai saistošajam regulējumam (GDPR, EHDS, DPA u.c.); Atzīti kiberdrošības sertifikāti, piem., ISO/IEC 27001	Datu izolācija starp projektiem; Piekļuves kontroles mehānismi, kas atbalsta MFA, lietotāju tiesību iestatīšanu, auditāciju; Atbilstība normatīvajam datu kopai saistošajam regulējumam (GDPR, EHDS, DPA u.c.); Atzīti kiberdrošības sertifikāti, piem., ISO/IEC 27001
Zinātniskai darbībai pielāgotas federētas mākoņpakalpojumu platformas	Pirms izmantošanas jāveic izvērtējums par: Datu rezidenci atbilstoši normatīvajam regulējumam; Datu izolācija starp projektiem; Piekļuves kontroles mehānismi, kas atbalsta MFA, lietotāju tiesību iestatīšanu, auditāciju; Atbilstība normatīvajam datu kopai saistošajam regulējumam (GDPR, EHDS, DPA u.c.); Atzīti kiberdrošības sertifikāti, piem., ISO/IEC 27001	Pirms izmantošanas jāveic izvērtējums par: Datu rezidenci atbilstoši normatīvajam regulējumam; Datu izolācija starp projektiem; Piekļuves kontroles mehānismi, kas atbalsta MFA, lietotāju tiesību iestatīšanu, auditāciju; Atbilstība normatīvajam datu kopai saistošajam regulējumam (GDPR, EHDS, DPA u.c.); Atzīti kiberdrošības sertifikāti, piem., ISO/IEC 27001	Pieļaujama tikai tad, ja risinājums ir sasaistīts ar kontrolētu apstrādes vidi, skatīt sadaļu 4 Pirms izmantošanas jāveic izvērtējums par: Datu rezidenci atbilstoši normatīvajam regulējumam; Datu izolācija starp projektiem; Piekļuves kontroles mehānismi, kas atbalsta MFA, lietotāju tiesību iestatīšanu, auditāciju; Atbilstība normatīvajam datu kopai saistošajam regulējumam (GDPR, EHDS, DPA u.c.); Atzīti kiberdrošības sertifikāti, piem., ISO/IEC 27001
Drošas apstrādes vide	Jāizmanto individuālas lietotāju identitātes un MFA. Datu imports un eksports jāveic tikai caur kontrolētiem kanāliem. Piekļuvei un galvenajām darbībām ir jāveic žurnalēšana.	Papildus 2. līmeņa prasībām: Interneta piekļuve jāierobežo pēc noklusējuma. Jānodrošina tikai apstiprināts pieejamo programmu kopums. Jāierobežo datu kopēšanas,	Papildu 3. līmeņa nosacījumiem jāpiemēro papildu kontroles: minimāls lietotāju loks; ierobežota datu importēšana un eksportēšana, pilna darbību auditācija

Tehnoloģiskā pieeja	2. līmeņa dati	3. līmeņa dati	4. līmeņa dati
	Detalizētāk skatīt sadaļu 4	lejupielādes un cita veida nekontrolēta datu iznešana. Detalizētāk skatīt sadaļu 4	dažādu projektu loģiskā izolācija, ārpus vides drīkst iziet tikai apstiprināti neaizsargāti dati vai agregēti rezultāti. Detalizētāk skatīt sadaļu 4
Personīgi vai citi personīgi pārvaldīti risinājumi	Neatbalstīt aizsargājamu datu apstrādei, glabāšanai vai kopīgošanai. Skaidri aizliegt iekšējā kārtībā un, kur iespējams, tehniski ierobežot izmantošanas iespējas.	Neatbalstīt aizsargājamu datu apstrādei, glabāšanai vai kopīgošanai. Skaidri aizliegt iekšējā kārtībā un, kur iespējams, tehniski ierobežot izmantošanas iespējas.	Neatbalstīt aizsargājamu datu apstrādei, glabāšanai vai kopīgošanai. Skaidri aizliegt iekšējā kārtībā un, kur iespējams, tehniski ierobežot izmantošanas iespējas.

Materiāls izstrādāts projekta «Atbalsts atvērtās zinātnes ieviešanai praksē, kā arī izveidoti risinājumi zinātnes datu koplietošanai un dalībai ES atvērtajā zinātnes mākonī» ietvaros (ANM projekta Nr. 2.1.3.1.i) ar Eiropas Savienības Atveseļošanas fonda un Latvijas valsts finansiālo atbalstu