Radni dokument o „Pametnim gradovima”

Usvojeno na 70. sjednici 29. - 30. Studenoga 2022.,
pisani postupak prije 71. sjednice 7. i 8. lipnja 2023.

1. Uvod

Gradovi su ključni za ljudski procvat. Aristotel je u svojoj *Politici* slavno rekao da je „ljudsko biće po prirodi životinja namijenjena gradu”1 i da grad postoji ne samo radi promicanja trgovine ili sprječavanja nepravde, već prije svega zbog toga što svojim građanima daje „potpun i samodostatan život”2.

Gradovi diljem svijeta usvajaju novu i inovativnu obradu kako bi postigli svoje ciljeve. To bi moglo uključivati uvođenje novih tehnologija ili usvajanje nove obrade s postojećim podacima. Putovanje prema stvaranju „pametnih” ili „povezanih” gradova zahtijeva smisleno upravljanje podacima od samog početka te danas kako bi se održalo povjerenje građana i pojedinaca koji posjećuju grad.

Pametni gradovi mogu uključivati brojne aktere i aktivnosti obrade. Ovim se dokumentom ne nastoje definirati pametni gradovi; umjesto toga, istražuje se tema digitalizacije gradova kao procesa u tri faze prikupljanja podataka, analize podataka i odlučivanja. U nastavku su prikazani neki primjeri prakse u navedenim fazama:

- 1 Aristotel, *Politika*, I.2 1253a3, trans. Joe Sachs. Indianapolis: Hackett, 2012.
- 2 Ibid., III.9 1280b30 – 33.

E-pošta:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Radnu skupinu podupiru Povjerenici za zaštitu podataka i neovisni stručnjaci iz zemalja diljem svijeta kako bi se poboljšala privatnost i zaštita podataka u tehnologiji.

Tajništvo
Savezni Povjerenik za zaštitu podataka i slobodu informiranja (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Telefon + 49/228 99/7799 1404

Prikupljanje podataka:

- Senzorske mreže kao što je internet stvari (IoT)
- Slike koje proizvodi videonadzor, dronovi itd.
- Ponovna uporaba podataka u posjedu javnih tijela[3], općina[4], i drugih partnera[5]
- Podaci prikupljeni od javnih komunikacijskih mreža kao što su Wi-Fi mreže javnog prijevoza.
- Podaci prikupljeni iz usluga koje nudi općina, kao što su najam bicikala ili skutera

Analiza podataka:

- Podudaranje podataka
    - Kombiniranje sadržaja dvaju skupova podataka kako bi se dobio novi uvid. Na primjer, upotreba podataka pametnih termostata i skupova podataka o socijalnim koristima kako bi se identificirala kućanstva u oskudici goriva.

- Umjetna inteligencija
    - Korištenje računala za obavljanje zadataka koji obično zahtijevaju ljudsku inteligenciju. Na primjer, upravljanje protokom prometa putem podataka prikupljenih kroz prometni sustav.
- Profiliranje
    - Korištenje osobnih podataka za procjenu ili predviđanje aspekata koji bi se mogli odnositi na fizičku osobu. Na primjer, korištenje profiliranja za predviđanje lokacije ili kretanja osobe kroz grad.
- Digitalni blizanci
    - Izgradnja digitalnog prikaza grada, precizno mapiranje fizičkog grada za eksperimentiranje novih politika ili procjenu predloženog urbanog razvoja.

Odluka:

- Upravljanje gradskim resursima kao što je javni prijevoz
- Upravljanje gradskim funkcijama ili postupcima kao što je kontrola prometa
- Ostvarenja koja gradovi upotrebljavaju kao dokaz za daljnje odluke, npr. donošenje politika o fondu socijalnih stanova ili socijalnim uslugama

---

3 Pod tijela javne vlasti misli se na tijelo koje pruža javnu uslugu, kao što je obrazovna ustanova ili agencija za davanje socijalnih naknada.
4 Pod općinom misli se na gradsko upravljačko tijelo.
5 Pod partnerima misli se na svakog suradnika s kojim grad može raditi. To bi mogli biti podizvođači, gradovi s kojima surađuju, usluge u gradu koje dijele podatke s gradskom upravom. Nastavlja se koristiti fraza partnera kao skraćenica za različite vrste aktera s kojima gradovi surađuju u projektima pametnih gradova.

Svaka od tih faza uključuje neki oblik izazova vezano uz zaštitu podataka i privatnosti. Od zakonitosti, pravednosti i transparentnosti do sigurnosti i integriteta te prava pojedinaca. Postoji širok raspon namjena za koje grad može usvojiti tehnologiju. Od upravljanja prometom do upravljanja socijalnom skrbi, potrošnje energije i urbanističkog planiranja putem digitalnih blizanaca. Usvajanje nove tehnologije ili obrada od strane grada u bilo koju od tih ilustrativnih svrha također otvara pitanja o interakciji s drugim pravima i slobodama.

U ovom radu prikazan je niz načela zaštite podataka i privatnosti koja se odnose na svaku od tih faza korištenja podataka u kontekstu grada. Ta načela predstavljaju neke od faza tehničke i integrirane zaštite podataka. Čitateljima može biti korisno istražiti daljnja područja tehničke i integrirane zaštite podataka te razmotriti njihovu važnost u pametnom gradskom kontekstu[6]. Ovaj rad razmatra rizike koji postoje obzirom na pojedini tematski skup načela, pruža ilustrativnu studiju slučaja i završava preporukama za gradske vlasti, regulatore i privatni sektor koji su uključeni u pružanje usluga temeljenih na podacima.

2. Odgovornost i upravljanje

Kako bi se postigla i dokazala usklađenost sa svim načelima zaštite podataka i zaštite prava pojedinaca, prije početka bilo kakve obrade gradovi i njihovi partneri trebali bi osigurati da provode strogu procjenu odgovornosti i upravljanja, uključujući, prema potrebi, procjenu učinka na zaštitu podataka. Postupak bi trebao uključivati timove za upravljanje podacima, kao što je službenik za zaštitu podataka, u ranoj fazi. Ključno donošenje odluka odvija se u početnim fazama, što može znatno utjecati na opseg upravljanja i uspostavu učinkovitih mjera. Ako se taj proces ne slijedi, postoji rizik da se u nove inicijative postupaka obrade od strane pametnih gradova ne ugradi odgovarajuća usklađenost sa zaštitom podataka, što uzrokuje društvene štete kao što su šteta za informacije i javni diskurs.

Jedno od ključnih pitanja bit će pitanje odnosi li se obrada na pojedince koji se mogu identificirati. Mogućnost utvrđivanja identiteta trebala bi biti pitanje vezano uz konkretnu obradu, ali i u vezi s povezanom obradom. Na primjer, pri odlučivanju hoće li instalirati nove senzore za mjerenje stope koraka na javnom mjestu, grad bi trebao odgovoriti na pitanje prikupljaju li senzori podatke koji se izravno mogu identificirati. Također bi trebali razmotriti uzrokuje li druga tehnologija koja djeluje na istom javnom mjestu promjenu u

6 Smjernice 4/2019 o članku 25. tehnička i integrirana zaštita podataka, Europski odbor za zaštitu podataka

mogućnosti utvrđivanja identiteta, pri čemu bi kombinacija novih senzora i postojećih sustava (npr. kamere zatvorenog kruga) mogla omogućiti neizravnu identifikaciju pojedinaca.

Gradovi bi trebali šire razmotriti pitanje prepoznatljivosti s obzirom na to da se obrada kreće od faze prikupljanja do faze analize. Razmotrite koja se obrada podataka odvija u fazi analize? Hoće li postojati podudarnost podataka koja bi mogla stvoriti puteve za utvrđivanje identiteta? Je li razdoblje pohrane takvo da će se daljnjim prikupljanjem omogućiti utvrđivanje obrazaca kretanja pojedinaca?

Navedena rasprava o identifikaciji definira nužan prostor za upravljanje. Ako gradovi zaključe da će obrada uključivati identificirane pojedince ili pojedince koji se mogu identificirati, postupak upravljanja trebao bi se orijentirati prema relevantnim standardima zaštite podataka i upravljanjem privatnosti. To uključuje provedbu procjene učinka kako bi se utvrdili i ublažili rizici za pojedince zbog obrade. Procjena učinka trebala bi uključivati i razmatranje učinka na druga ljudska prava i slobode.[7]

Aplikacije za pametne gradove uvijek bi trebale biti nadahnute pravednošću. Podaci loše kvalitete ili podaci koji ne odražavaju raznolikost skupina stanovništva mogu dovesti do nepravednih ili diskriminirajućih odluka. Taj bi aspekt također trebalo ispitati i razmotriti tijekom procjene učinka. Konkretno, gradovi bi trebali procijeniti je li kvaliteta podataka koji se upotrebljavaju za donošenje odluka s mogućim učincima na prava i slobode pojedinaca primjerena i reprezentativna prema obilježjima stanovništva. Mnogi čimbenici mogu narušiti kvalitetu i reprezentativnost podataka. Na primjer, veličina uzorka populacije, jesu li pojedinci odustali od obrade ili su uložili prigovor na obradu ili su zahtijevali brisanje njihovih podataka. Ako gradovi ne mogu jamčiti najvišu kvalitetu podataka ili standarde reprezentativnosti podataka u pogledu svrhe obrade, trebali bi se suzdržati od daljnje upotrebe tih podataka u tu svrhu.

Osim toga, uspostava odgovarajućih mehanizama transparentnosti za informiranje pojedinaca o obradi i uvođenju tehničkih i organizacijskih mjera kako bi se osiguralo da se prakse zaštite privatnosti uspostave u najranijoj mogućoj fazi dio je obveza odgovornosti.

Ta bi se rasprava trebala odvijati između grada i svih partnera koji sudjeluju u obradi. To je važno kako bi se osiguralo da grad dodjeljuje odgovarajuće uloge i odgovornosti među subjektima uključenima u obradu. Ako je sustav namijenjen isključivo za gradsku upotrebu, rasprave se mogu usredotočiti na dizajn sustava. To mora uključivati kontrole

7 Modernizirana Konvencija za zaštitu pojedinaca glede obrade osobnih podataka.

pristupa za sve timove koji pristupaju podacima. Ako to uključuje pružanje usluga od strane partnera iz industrije, kao što je analiza podudaranja podataka, tada je uz oblikovanje dizajna sustava potrebna daljnja rasprava o upravljanju podacima, uključujući odnos voditelja obrade i izvršitelja obrade ili zajedničko vođenje obrade. To je nužno jer pružanjem usluge partner može odrediti sredstva i svrhu usklađivanja podataka, ili koristiti vlasničke podatke koje posjeduje ili dodati vlastite podatke. To mijenja prirodu odnosa i zahtijeva zajedničke mehanizme upravljanja.

Postupci upravljanja i odgovornosti moraju se dovršiti prije obrade kako bi se osiguralo da su uspostavljeni odgovarajući sustavi, uključujući tehničke zaštitne mjere, te dogovor o ulogama i odgovornostima između stranaka. Ishod postupka odgovornosti trebao bi se i dalje redovito preispitivati kako bi se osiguralo da i dalje bude relevantan u opisu obrade, procjene rizika i primjene mjera ublažavanja. Navedeno bi trebalo preispitati i kada se u nadziranom području ili u relevantnoj službi za grad uvede nova tehnologija ili inicijativa. Na primjer, novi uređaj za praćenje uveden na javni trg s kontinuiranim prikupljanjem podataka ili novi analitički sustavi za upravljanje potražnjom za javnim prijevozom.

Regulatorna tijela mogu pomoći u raspravi o upravljanju izradom smjernica o uspostavi postupaka odgovornosti i upravljanja. Bilo bi korisno izraditi smjernice o scenarijima u kojima je uključeno više sudionika, usluga i tehnologija.

2.1 Primjer odgovornosti: Enschede

U rujnu 2017. općina Enschede odlučila je započeti 24/7 Wi-Fi praćenje u gradskom centru[8]. Njegova je svrha bila mjerenje učinkovitosti općinskih ulaganja s obzirom na odgovorna sredstva. Sklopila je ugovor s partnerom za isporuku, koji je zatim ugovorio drugu stranu za instalaciju i održavanje senzora te prikupljanje i potvrđivanje podataka koje su prikupili senzori.

Informacije prikupljene i privremeno pohranjene na senzoru uključivale su MAC- adrese, datum i vremensku oznaku izloženosti, jačinu signala. Senzor je poslao informacije središnjem poslužitelju, s oznakom MAC-adresa i dodanim ID senzora. Poslužitelj je čuvao prikupljene informacije u razdoblju od 6 do 7 mjeseci. Od početka 2019. partner je uspostavio dodatne mjere anonimizacije skraćivanjem dijela raspršene MAC adrese. Općina je naredila partneru za isporuku da u 2020. isključi senzore.

Općina je tvrdila da su podaci dovoljno anonimizirani tako da nije bilo obrade osobnih

8 AP (Nizozemska) – Gemeente Enschede – GDPRHub

podataka. Općina je tvrdila i da u ovom slučaju nije voditelj obrade podataka.

AP (nizozemsko tijelo za zaštitu podataka) zaključilo je da odabrana anonimizacijska metoda skraćivanja dijela raspršene MAC adrese ne isključuje u dovoljnoj mjeri rizik od izdvajanja, povezivanja ili utvrđivanja identiteta osobe.9 AP je donio odluku na temelju prikupljanja pseudonimnog identifikatora + vremenski žig + informacije o lokaciji (dostupne putem identifikacijske oznake senzora). Kao rezultat toga, podaci koje je obradila općina činili su osobne podatke. Prema AP-u, općina je bila voditelj obrade jer je odlučila o sredstvima i svrhama obrade osobnih podataka izdavanjem naloga o pojedinostima obrade.

2.2 Preporuke o odgovornosti i upravljanju:

Gradovi bi trebali jasno dokumentirati opseg njihove obrade u svim svojim službama.

Gradovi bi trebali osigurati da podaci koji se upotrebljavaju u odlukama budu primjereni svrsi obrade i reprezentativni za obilježja stanovništva.

Gradovi bi trebali uspostaviti tehničke i organizacijske mjere za uspostavu odgovarajućeg upravljanja i zaštitnih mjera za obradu podataka.

Gradovi bi trebali provesti procjene učinka prije početka obrade kako bi utvrdili i ublažili rizike te razmotrili učinak na druga prava i slobode tijekom procjene.

Procjene učinka trebale bi se redovito preispitivati i grad bi ih trebao u potpunosti preispitati kada se nova tehnologija uvede u područje koje se prati ili u relevantnu gradsku službu.

Gradovi bi trebali uključiti svoje timove za upravljanje podacima u ranoj fazi i savjetovati se s njima tijekom cijelog postupka.

Gradovi bi trebali provesti odgovarajuća savjetovanja s javnošću i drugim relevantnim dionicima u okviru postupka odgovornosti i upravljanja.

Regulatorna tijela trebala bi izraditi smjernice o mjerama odgovornosti i upravljačkim strukturama, uključujući smjernice o obradi s više uključenih sudionika, usluga i tehnologija.

9 Mišljenje WP29 05/2014 o tehnikama anonimizacije

3. Smanjenje količine podataka

Načelom smanjenja količine podataka nastoji se osigurati da voditelji obrade prikupljaju samo podatke koji su relevantni, primjereni i nužni za određenu zakonitu svrhu. U kontekstu pametnog grada, svrha je često razumjeti trendove, kao što je gustoća prometa, iz „ptičje perspektive". Ove svrhe često uključuju traženje procjene podataka u zbirnom obliku.

Ako je cilj analiza trendova, smanjenje količine podataka zahtijeva sakupljanje i uklanjanje identifikatora što je prije moguće u fazi prikupljanja. Time se smanjuje identifikacija u fazi analize. Ako to ne učinite, postoji rizik od prekomjernog prikupljanja osobnih podataka i stvaranja nepotrebnog uplitanja u privatnost građana.

Kako bi se smanjila količina podataka u praksi, gradovi bi trebali jasno definirati podatke potrebne za postizanje posebne svrhe obrade. To se mora dogoditi prije početka obrade. Definiranje svrhe u fazi projektiranja znači da sustavi imaju bolje izglede za odražavanje te određene svrhe. Time bi se također trebalo omogućiti uključivanje prakse smanjenja količine podataka u sam sustav prikupljanja. Na primjer, nabavom senzora koji prikupljaju samo određene podatke ili uklanjaju identifikatore prije slanja podataka na analizu. Također bi trebale postojati jasne politike povezane s automatiziranim brisanjem prikupljenih podataka kada više nisu potrebni a u svrhu smanjenja rizika od gubitka podataka.

Postizanje tog sakupljanja moglo bi uključivati usvajanje tehnologije za poboljšanje privatnosti (PET-ovi; Privacy Enchancing Technologies). PET-ovi mogu pomoći u prikazivanju podataka anonimiziranim ili pseudonimiziranim. Usvajanje tih tehnologija u ranoj fazi ciklusa obrade predstavlja dobru praksu tehničke i integrirane zaštite privatnosti. Čineći to na način da se funkcionalnost ugrađuje u sustav na takav način da je obvezna osigurava se da će obrada uvijek pokazati standarde smanjenja količine podataka.

Nadzorna tijela za zaštitu podataka mogla bi imati koristi pružanjem smjernica o upotrebi anonimizacije i PET-ova u obradi. U tim bi se smjernicama mogle predložiti dostupne tehnike za smanjenje rizika od identifikacije pojedinaca na prihvatljivu razinu. Smjernice mogu pomoći u oblikovanju vrsta proizvoda koje industrija plasira prema gradovima i obrade koju industrija ugrađuje u svoje proizvode kako bi osigurala uspostavu smanjenja količine podataka.

3.1 Primjer smanjenja količine podataka: Wi-Fi prikupljanje podataka – Prijevoz za London (Transport for London – TfL)

3.2 Prijevoz za London (TfL), tijelo nadležno za prijevoz koje upravlja svakodnevnom londonskom mrežom javnog prijevoza, nastojalo je bolje razumjeti kako se klijenti kreću kroz stanice10. Nisu morali identificirati određene pojedince kako bi postigli takvo razumijevanje.

Kako bi ostvario svoj cilj, TfL je odlučio prikupljati podatke o Wi-Fi vezama s više stanica. Wi-Fi veza „pruža daleko bolje razumijevanje kako se korisnici kreću kroz stanice". Ova metoda značila je prikupljanje lokacije uređaja na Wi-Fi mreži, u skladu s definicijom osobnih podataka.

Ako uređaj pronađe Wi-Fi mrežu koja je poznata uređaju, automatski će se spojiti na tu mrežu. Ako uređaj pronađe nepoznate mreže, navesti će ih u postavkama uređaja pojedinca kako bi pojedinac mogao odlučiti hoće li se spojiti.

Svi prikupljeni podaci automatski se raspršuju pomoću revolving kriptografske funkcije. To, prema TfL-u, osigurava da se ne može identificirati nijednu osobu. Sustav je to učinio odmah nakon prikupljanja podataka.

TfL nije imao namjeru uskladiti podatke o Wi-Fi vezama s drugim podacima o pojedincima koje nadležno tijelo posjeduje (npr. podaci o putnoj kartici), a zbog neposrednog postupka pseudonimizacije ne postoji način da se to sustavno učini, prema TfL-u.

TfL je koristio zbirne podatke o Wi-Fi vezama kako bi shvatio koliko su prometne postaje londonske podzemne željeznice tijekom dana. Ove informacije su pomogle pojedincima planirati svoje putovanje, kao i doprinijeti razumijevanju korištenja stanica od strane TFL-a.

3.3 Preporuke za smanjenje količine podataka

Gradovi bi trebali jasno definirati podatke potrebne za postizanje svrhe i razviti sustave koji odražavaju tu svrhu.

Gradovi bi trebali osigurati da sustavi uvijek svedu podatke na najmanju moguću mjeru uključivanjem tehničkih i organizacijskih mjera u prikupljanje osobnih podataka što je prije moguće.

Gradovi bi trebali osigurati da mjere za smanjenje količine podataka budu prisutne

10 Wi-Fi Prikupljanje podataka – Transport for London (tfl.gov.uk)

tijekom cijelog životnog ciklusa, uključujući provedbu odgovarajućih razdoblja zadržavanja i uspostavu sigurnih postupaka brisanja.

Regulatorna tijela trebala bi gradovima i industriji pružiti smjernice o metodama za smanjenje količine podataka, uključujući sakupljanje.

4. Ograničenje svrhe

Gradovi imaju višestruku ulogu u životu svojih građana, od upravljanja prometom do javne sigurnosti te obrazovanja i kontrole emisija. Tehnički sustavi trebali bi odražavati različite podatke i različite svrhe razdvajanjem aktivnosti obrade. Trebalo bi uspostaviti organizacijske mjere kako bi se osiguralo da osoblje ne može podatke prikupljene u jednu svrhu upotrebljavati u drugu svrhu bez odgovarajuće procjene, dokumentacije i pravne osnove.

Trebalo bi jasno priopćiti svrhu obrade na mjestu prikupljanja, a mjere upravljanja moraju odražavati tu svrhu. Ako se u sustavima za obradu ne uspostavi odgovarajuće ograničenje svrhe, postoji rizik od razmjene podataka izvan izvorne svrhe. Navedeno uzrokuje štetu pojedincima zbog gubitka kontrole nad podacima.

U nekim se situacijama podaci mogu upotrebljavati u drugu svrhu, na primjer, u fazi analize skupovi podataka iz više izvora mogu se kombinirati, uspoređivati ili sparivati za potrebe utvrđivanja osoba koje imaju pravo na socijalne naknade. To predstavlja visok rizik od gubitka kontrole pojedinaca nad osobnim podacima, a moglo bi pridonijeti i nedostatku autonomije ili manipuliranju izborima ljudi. Obrada bi se trebala nastaviti samo ako je nova svrha u skladu s izvornom svrhom ili ako pojedinac valjano pristane ili ako voditelj obrade jasno utvrdi definiranu pravnu obvezu.

Voditelj obrade trebao bi provesti procjenu kompatibilnosti kako bi utvrdio je li plan za upotrebu ili otkrivanje osobnih podataka u dodatnu svrhu kompatibilan. Voditelj obrade trebao bi pojedincima pojasniti tu novu svrhu kako bi počeo smanjivati rizike od gubitka kontrole nad osobnim podacima. Voditelj obrade trebao bi procijeniti pravednost nove obrade, čime se počinje ukazivati na rizik manipulacije i gubitak autonomije.

Industrija bi trebala izgraditi sustave sa fleksibilnosti za uspostavu različitih organizacijskih mjera i donijeti tehničke mjere za ispunjavanje standarda tehničke i integrirane zaštite privatnosti. To bi moglo značiti uspostavu kontrola pristupa temeljenih na snažnim ulogama kako bi samo timovi koji rade za određenu svrhu mogli pristupiti prikupljenim podacima. Tehničke mjere mogle bi uključivati log funkcije kojima se bilježi tko pristupa tim podacima, čime se omogućuje provođenje revizija u okviru

preispitivanja.

4.1 Primjer ograničenja svrhe: Pametne kuće

Sve više socijalnih stanova koje osiguravaju javna tijela i gradovi imaju ugrađene senzore koji prate razinu vlage. Svrha je toga osigurati da pruženi smještaj bude siguran i zdrav za stanara te omogućiti proaktivno održavanje kako bi se riješili novi problemi prije nego što postanu opsežniji i skuplji za pružatelja usluga.

Dobavljači tih sustava također nude aplikacije za bolje informiranje stanara o potrošnji energije unutar kuće. Podaci bi također mogli pružiti uvid u podobnost stanara za socijalne naknade. Na primjer, podaci dosljedno niske temperature mogli bi upućivati na kućanstvo koje je u oskudici goriva. Tada bi javna tijela mogla tom kućanstvu staviti na raspolaganje socijalne naknade.

U ovom primjeru postoje tri različite svrhe: održavanje smještaja za socijalno stanovanje; informiranje stanara o njihovoj potrošnji energije; i utvrđivanje prihvatljivosti za socijalne naknade. Izvorna svrha u ovom primjeru je održavanje smještaja za socijalno stanovanje, dodatne svrhe zahtijevaju procjenu njihove spojivosti s tom izvornom svrhom. Ako nova svrha nije u skladu s izvornom svrhom, mora postojati jasna obveza ili funkcija utvrđena zakonom kako bi se omogućila ta nova svrha ili valjana privola pojedinca.

Intervencije u živote pojedinca za socijalne naknade, čak i ako se smatraju pozitivnima, bitno su drugačija svrha od praćenja stanja doma kako bi se osigurali pravovremeni popravci. U ovom primjeru treća svrha trebala bi uspostaviti jasnu zakonsku obvezu ili imati privolu stanara prije početka obrade.

Nadalje, potrebno je obavijestiti pojedinca o tim svrhama i, prema potrebi, prikupiti privolu.

Dizajn sustava također bi trebao odražavati te različite svrhe. Na primjer, pružatelj usluga stanovanja trebao bi primiti podatke koji ukazuju na stanje kuće, što možda uopće nije osobni podatak. Sučelje aplikacije trebalo bi korisniku pružiti odgovarajuće i relevantne podatke o njegovoj potrošnji energije. Potrebno je uspostaviti program razmjene podataka između pružatelja usluga stanovanja i tima za socijalnu potporu ako odluče ostvariti treću svrhu. To može uključivati neke podatke koji se podudaraju sa stambenim podacima i osobnim podacima stanara.

4.2 Preporuke za ograničenje svrhe

Gradovi bi trebali osigurati da podatke obrađuju samo u utvrđene svrhe usvajanjem

tehničkih i organizacijskih mjera. Gradovi bi trebali dokumentirati te svrhe i staviti dokumentaciju na raspolaganje pojedincima.

Gradovi bi trebali provoditi procjene kompatibilnosti kada upotrebljavaju podatke u svrhe različite od prvotno prikupljenih.

Gradovi bi trebali poduzeti odgovarajuće korake upravljanja nakon procjene kompatibilnosti, uključujući, prema potrebi, traženje privole pojedinca za novu svrhu i sklapanje sporazuma o razmjeni podataka među sudionicima.

Industrija bi trebala izgraditi sustave koji imaju fleksibilnost za utvrđivanje organizacijskih mjera i donošenje tehničkih mjera kako bi se zadovoljilo ograničenje svrhe.

5. Integritet i povjerljivost

Širenje aktivnosti obrade u gradovima dovodi do povećanja mjesta prikupljanja, količine prikupljenih podataka, a u nekim slučajevima i proširenja pohrane tih podataka. To stvara nove izazove za održavanje integriteta i povjerljivosti prikupljenih osobnih podataka. Mreže koje se temelje na senzorima posebno imaju važnu ulogu u povećanju mogućnosti prikupljanja podataka za gradove, a istodobno su dosljedan izvor zabrinutosti za sigurnosne standarde.[11]

Integritet i povjerljivost sustava obrade predstavljaju potencijalni problem. Gradovi bi trebali osigurati da aktivnosti nabave uključuju rasprave o integritetu i povjerljivosti. Gradovi bi mogli podržati te rasprave o nabavi utvrđivanjem standarda za procjenu predloženih sustava provedbe standarda privatnosti. Od nabave nadalje potrebno je osigurati odgovarajuća sredstva za kontinuiranu procjenu integriteta sustava kako bi se osiguralo da timovi rješavaju nove rizike i rizike u nastajanju.

Industrija ima ključnu ulogu u integritetu i povjerljivosti sustava obrade. Razvoj sustava koji se temelje na senzorima trebao bi pokazati cjelovitost i povjerljivost, uz istodobno dovoljno kapaciteta za primanje sigurnosnih ažuriranja nakon utvrđivanja budućih ranjivosti.

5.1 Integritet i povjerljivost (primjer): Nove zakonodavne inicijative i međunarodni konsenzus o sigurnosti interneta stvari (IoT)

Postoje razne inicijative iz cijelog svijeta koje pokazuju potrebu da se osigura sigurnost

11 Načela kibernetičke sigurnosti povezanih mjesta – NCSC.GOV.UK

IoT uređaja. Cilj je Ujedinjenog Kraljevstva vezano uz sigurnost proizvoda i telekomunikacija[12] poboljšati kibernetičku sigurnost usmjerenu na potrošače, s posebnim naglaskom na sigurnost proizvoda. To uključuje zabranu upotrebe zadanih lozinki, zahtjev da proizvođači upravljaju izvješćivanjem o sigurnosnim ranjivostima i zahtjev da potrošače na prodajnom mjestu obavijeste o minimalnom razdoblju u kojem će proizvod dobiti sigurnosna ažuriranja.

Nadalje, sudionici iz cijele industrije, akademske zajednice i donošenja političkih akata prepoznaju potrebu za poboljšanjem sigurnosti IoT uređaja. Zajednička izjava o podršci vezano uz sigurnost za potrošački IoT uređaj [13] poziva na širok razvoj osnovnih sigurnosnih standarda IoT-a kako bi se osigurale osnovne sigurnosne značajke u svakom povezanom IoT uređaju. Gradovi bi trebali biti oprezni pri usvajanju IoT uređaja za pružanje usluga općina. Građani nemaju alternativu sustavu koji nudi grad te bi stoga gradovi trebali moći dokazati provedbu potrebnih tehničkih, organizacijskih i pravnih sredstava za osiguravanje sigurnosti podataka IoT uređaja.

5.2 Preporuke vezane uz integritet i povjerljivost

Gradovi bi trebali uspostaviti standarde procjene za nabavu novih sustava kako bi se utvrdila provedba pitanja privatnosti.

Gradovi bi trebali zahtijevati dokazivanje sigurnosnih standarda prije nabave sustava obrade.[14]

Gradovi bi trebali uspostaviti revizijske prakse kojima se redovito testiraju svi dijelovi sustava za obradu podataka tijekom cijelog životnog ciklusa podataka kako bi se osiguralo da se njime održavaju potrebne razine integriteta i povjerljivosti.

Industrija bi trebala osigurati da njihovi proizvodi odražavaju najbolje prakse u industriji, kao što je mogućnost primanja sigurnosnih nadogradnji, provođenja politike otkrivanja ranjivosti te da se ne koriste univerzalne zadane lozinke.

12 Sigurnost proizvoda i telekomunikacijska infrastruktura (PSTI)– GOV.UK (www.gov.uk)
13 Zajednička izjava o potpori vezano uz sigurnost potrošačkih IoT uređaja | Cyber Tech Accord (cybertechaccord.org)
14 Na primjer, vidjeti preporučene prakse IEEE-a za razmatranje privatnosti u vezi tehnologije IEEE 802 (https://1.ieee802.org/security/802e/).

6. Pravo na informaciju

Transparentnost obrade jedinstven je izazov za pametne gradove. Faza prikupljanja podataka često je pasivna. Pasivno u ovom smislu znači da se prikupljanje tehnički može dogoditi bez individualne prijave za prikupljanje ili da se ponovna upotreba prethodno prikupljenih podataka za novu inicijativu može dogoditi bez da se pojedinac ikad obavijesti. Te su aktivnosti, kada se njima rukuje bez odgovarajuće transparentnosti, nevidljiva obrada – obrada podataka koji nisu izravno dobiveni od pojedinca – s povezanim štetama gubitka kontrole nad podacima za pojedince, ali i društvenim štetama povezanima s gubitkom povjerenja u grad i druge institucije radi poštenog i transparentnog postupanja s njihovim podacima.

Iako je teško informirati pojedince o pametnoj gradskoj obradi, to je ostvarivo. Gradovi bi trebali poduzeti korake kako bi bolje informirali građane o vrsti obrade koja se odvija.15 U nekim okolnostima prikupljeni podaci bit će osobni podaci te će postojati zakonska obveza obavješćivanja pojedinaca o prikupljanju. U drugim okolnostima, ako se podaci ne mogu izravno ili neizravno identificirati, postoji etičko pitanje o tome kako izgleda dobra praksa za usvajanje nove i inovativne obrade.

Gradovi bi trebali razmotriti kako informiraju građane o svakoj aktivnosti obrade i opsegu obrade diljem grada. Gradovi bi na mjestu prikupljanja trebali staviti na raspolaganje informacije za određenu aktivnost obrade. Pojedinci bi, prema potrebi, trebali dobiti informacije o naknadnim fazama analize i donošenja odluka koje govore o svrsi prikupljanja.

Gradovi imaju jedinstvene mogućnosti za metode komunikacije u svrhu informiranja građana o širim ciljevima. Oni mogu imati priliku komunicirati o projektima na prometnim lokacijama javnog prijevoza, širiti informacije kroz škole ili koristiti lokalne vijesti kako bi informirali građane o svojim širim namjerama. Gradovi također mogu održavati rasprave u svojim institucijama o inicijativama za pametne gradove te se mogu savjetovati i prikupljati mišljenja članova zajednice.

Neki su gradovi istražili javne registre aktivnosti obrade. U sklopu razvoja pametnog grada Sidewalk Labsa u Torontu namjeravalo se uspostaviti registar uređaja. Registar bi bio javno dostupan skup svih uređaja za prikupljanje podataka – koje su podatke prikupili, zašto, kako i tko ih je prikupio. Amsterdam Algorithm Register16 je inicijativa

15 Također potrebno je imati na umu da postoje inovativni pristupi, jedan od primjera je projekt imec-SMIT-VUB za zaštitu podataka (https://smit.vub.ac.be/policy-brief-57-walkshops). Drugi je primjer Infrastruktura za zaštitu privatnosti interneta stvari koja mapira senzore interneta stvari u javnom prostoru, uključujući gradove kao što su Amsterdam i Bruxelles (https://www.iotprivacy.io).

16 Amsterdam Algoritmeregister –

grada Amsterdama da se na jednom mjestu navedu obrada algoritmima koji se trenutno događaju u gradu. Ako gradovi žele prihvatiti prilike za uvid u tehnologiju, potrebno je jednako prihvatiti veću razinu transparentnosti i podizanje svijesti koje tehnologija može pružiti.

Ti primjeri pokazuju jedinstvene mogućnosti za komunikaciju šire obrade. Međutim, ključno je prepoznati da u nekim okolnostima, u kojima gradovi prikupljaju osobne podatke, postoji potreba za priopćavanjem jasnih informacija pojedincima u trenutku prikupljanja. Te bi informacije trebale sadržavati pojedinosti o prikupljenim podacima, njihovoj svrsi, sudionicima uključenima u obradu i ključnim upravljačkim točkama kao što su trajanje zadržavanja i sve mjere za deidentifikaciju koje se provode. To je temeljna odgovornost kojoj je potrebna dovoljna pozornost, kao i istraživanje širih komunikacijskih mogućnosti.

6.1 Primjer transparentnosti prema građanima: TfL Wi-Fi praćenje

Vratimo se na primjer praćenja Wi-Fi mreže tvrtke Transport for London iz prethodnog odjeljka o smanjenju količine podataka. Tijekom pilot-faze TfL je prepoznao potrebu za obavješćivanjem građana o početnom prikupljanju podataka prije deidentifikacije. Pristupili su zadatku informiranja kupaca kroz niz različitih aktivnosti.

Tijekom pilot-faze TfL je usvojio slojevit pristup.[17] Tjedan prije pokretanja pilot-projekta TfL je objavio priopćenje za medije u kojem su navedeni opseg projekta i predviđene koristi. TfL je koristio Metro, lokalne novine, za objavljivanje pojedinosti projekta. Tijekom cijelog pilot-projekta bila je dostupna internetska stranica s dodatnim informacijama

Diljem pilot područja postavljeno je više od tri stotine velikih plakata, što je posebno važna aktivnost širenja informacija na mjestu prikupljanja. Zaposlenici na tim postajama također su imali sastanke/izvještaje o suđenju kako bi mogli odgovoriti na pitanja ili uputiti pojedince na izvore dodatnih informacija.

6.2 Preporuke o pravu na informiranje

Kao preduvjet za prikupljanje osobnih podataka gradovi bi trebali uspostaviti metode za pružanje smislenih informacija pojedincima prije prikupljanja.

Gradovi bi trebali pružiti javno dostupne informacije kojima se objašnjava opseg obrade diljem grada, uključujući treće strane uključene u obradu i njihove uloge.

17 Pregled pilot-projekta TfL WiFi – naši nalazi

7. Pojedinačna prava

Pravo pojedinaca da kontroliraju svoje osobne podatke odgovornost je gradova i njihovih partnera kao voditelja obrade osobnih podataka. To bi moglo uključivati pristup podacima, prigovor na obradu, ispravljanje činjeničnih pogrešaka ili brisanje podataka. Zbog višestrukih postupaka obrade koji bi mogli djelovati u pametnom gradu od ključne je važnosti da gradovi uspostave jasne i pristupačne postupke za ostvarivanje prava pojedinca.

Prava pojedinaca najbolje su ispunjena ako postoji jasno razumijevanje svih uključenih strana. To razumijevanje uključuje ulogu aktera u obradi podataka i razumijevanje tko je odgovoran za ostvarivanje prava pojedinca. Potreba za jasnoćom obuhvaća i pravo pojedinaca da su upoznati sa obradom svojih podataka i, prema potrebi, pravima koja imaju na te podatke.

Oni koji kontroliraju svrhu i sredstva obrade imaju odgovornost informirati pojedince o obradi i pravima koja se odnose na te podatke. Faza dizajna trebala bi omogućiti odgovore i dokumentiranje ovih pitanja i odražavati preporuke za odgovornost i upravljanje navedene u gornjem odjeljku o Odgovornosti.

Ako gradovi ugovaraju isporuku partnerima, kao što su pružatelji komunikacijskih usluga za javni Wi-Fi, možda će biti potrebno preuzeti zajedničku odgovornost za te uloge. Grad bi to trebao jasno navesti u dozvoli i sklapanju ugovora za tu uslugu. Ako grad prikuplja i koristi podatke putem te mreže i odlučuje o svrsi, snosit će isključivu odgovornost za individualna prava i u skladu s time uspostaviti politike i procese.

Regulatorna tijela mogu smisleno doprinijeti raspravi pružanjem smjernica gradovima za ostvarivanje pojedinačnih prava. Regulatorna tijela također mogu pružiti javno dostupne informacije o pojedinačnim pravima i njihovu ostvarivanju.

7.1 Primjer individualnih prava: Planovi gradova za povećanje individualne kontrole

Strateški okvir za digitalnu infrastrukturu u Torontu,[18] objavljen u ožujku 2022., uključuje predanost „digitalnoj autonomiji" koja, među ostalim, uključuje povećanje kontrole stanovnika nad prikupljanjem i dijeljenjem njihovih osobnih podataka. Iako je ovaj okvir još prekratko u uporabi da bi se izradio radni model, pokazuje namjeru gradova da prepoznaju snažniju predanost pravima pojedinaca.

18 Strateški okvir za digitalnu infrastrukturu (toronto.ca)

Helsinki je najavio da namjerava stvoriti 'Helsinki Profile dashboard'[19], gdje ljudi mogu centralno upravljati privolom za različite usluge. Helsinki je dio MyData Globalne mreže. Koncept upravljanja osobnim informacijama koji omogućuje ljudima da razumiju podatke prikupljene od njih i daju privolu za njihovo korištenje.

7.2 Preporuke o individualnim pravima

Gradovi bi trebali uspostaviti sustave koji su u skladu s individualnim pravima, osiguravajući da kupljeni proizvodi mogu zadovoljiti te potrebe.

Gradovi i partneri iz industrije koji zajednički provode projekte trebali bi se prije početka obrade zajedno baviti pitanjima upravljanja u vezi s pravima pojedinaca.

Regulatorna tijela trebala bi pružati smislene informacije o pravima građana u vezi s obradom osobnih podataka u inicijativama za pametne gradove.

8. Završne napomene

Opseg obrade osobnih podataka u gradovima i unutar njih vjerojatno će rasti. To je posljedica uvođenja novih tehnologija za prikupljanje i prilika za inovativnu upotrebu podataka kako bi se bolje odgovorilo na izazove modernih gradova. S tim povećanim opsegom dolazi i potreba za uspostavom politika i sustava za zaštitu osobnih podataka tijekom cijelog ciklusa prikupljanja – analize – odluke koja je navedena u gore navedenom Uvodu.

Predložene preporuke odražavaju odgovornosti koje proizlaze iz povećane obrade i mogućnosti koje gradovi imaju za poboljšanje povjerenja u tu obradu. To uključuje potrebu za jasnim utvrđivanjem uloga i odgovornosti sudionika uključenih u te projekte, smanjenje prikupljanja podataka na potrebne razine i osmišljavanjem sustava kojima se uspostavljaju smislena ograničenja u pogledu upotrebe podataka. Mogućnosti uključuju širenje svijesti o obradi na razini grada u korist javnosti, usvajanje novih praksi za poboljšanje privatnosti kako bi se omogućile odgovorne inovacije i bolje ostvarivanje prava građana u vezi s prikupljenim osobnim podacima.

Pametni gradovi su dugo u razvoju. Vidjeli smo različite oblike ove ideje, od područja postojećih gradova predanih tehnološkim tvrtkama do razvoja potpuno nenaseljenih zemljišta za nove gradove. Neke od tih ideja nikada nisu prešle fazu izrade nacrta. Ovi projekti postaju sve češći u gradovima u kojima danas živimo. To znači da naši osobni

19 Mikko Rusama, Helsinki: Pisanje pravilnika o osobnim podacima – Gradovi danas (cities-today.com)

podaci postaju sve aktivniji problem. Od ključne je važnosti uspostaviti mehanizme upravljanja kako bi se odrazila ta povećana obrada.

Iako će gradovi imati mnoge odgovornosti prilikom ostvarenja uspjeha u tim projektima, privatni sektor, regulatorna tijela i sami građani imat će ključnu ulogu u održavanju odgovornosti projekata za podatke koje obrađuju i pomažući im da ostanu usmjereni na čovjeka u njihovim rezultatima.

Sažetak preporuka

Gradovi

- Gradovi bi trebali provesti procjene učinka prije početka obrade kako bi utvrdili i ublažili rizike te razmotrili učinak na druga prava i slobode tijekom procjene.
- Gradovi bi trebali osigurati da podaci koji se upotrebljavaju u odlukama budu primjereni svrsi obrade i reprezentativni za obilježja stanovništva.
- Procjene učinka trebale bi se redovito preispitivati i grad bi ih trebao u potpunosti preispitati kada se nova tehnologija uvede u područje koje se prati ili u relevantnu gradsku službu.
- Gradovi bi trebali uključiti svoje timove za upravljanje podacima u ranoj fazi i savjetovati se s njima tijekom cijelog postupka.
- Gradovi bi trebali provesti odgovarajuća savjetovanja s javnošću i drugim relevantnim dionicima u okviru postupka odgovornosti i upravljanja.
- Gradovi bi trebali jasno definirati podatke potrebne za postizanje svrhe i razviti sustave koji odražavaju tu svrhu.
- Gradovi bi trebali osigurati da sustavi uvijek svedu podatke na najmanju moguću mjeru uključivanjem tehničkih i organizacijskih mjera u prikupljanje osobnih podataka što je prije moguće.
- Gradovi bi trebali osigurati da mjere za smanjenje količine podataka budu prisutne tijekom cijelog životnog ciklusa, uključujući provedbu odgovarajućih razdoblja zadržavanja i uspostavu sigurnih postupaka brisanja.
- Gradovi bi trebali osigurati da podatke obrađuju samo u utvrđene svrhe donošenjem tehničkih i organizacijskih mjera. Gradovi bi trebali dokumentirati te svrhe i učiniti ih dostupnima pojedincima.
- Gradovi bi trebali provoditi procjene kompatibilnosti kada upotrebljavaju podatke u

svrhu različitu od prvotno prikupljenih.

- Gradovi bi trebali poduzeti odgovarajuće korake upravljanja nakon procjene kompatibilnosti, uključujući, prema potrebi, traženje privole pojedinca za novu svrhu i sklapanje sporazuma o razmjeni podataka među sudionicima.
- Gradovi bi trebali uspostaviti procjenu standarda za nabavu novih sustava kako bi se utvrdila provedba pitanja privatnosti.
- Gradovi bi trebali zahtijevati dokazivanje sigurnosnih standarda prije nabave sustava obrade.
- Gradovi bi trebali uspostaviti revizijske prakse kojima se redovito testiraju svi dijelovi sustava za obradu podataka tijekom cijelog životnog ciklusa podataka kako bi se osiguralo da se njime održavaju potrebne razine integriteta i povjerljivosti.
- Gradovi bi trebali uspostaviti metode za pružanje smislenih informacija pojedincima u trenutku prikupljanja osobnih podataka.
- Kao preduvjet za prikupljanje osobnih podataka gradovi bi trebali uspostaviti metode za pružanje smislenih informacija pojedincima prije prikupljanja.
- Gradovi bi trebali pružiti javno dostupne informacije kojima se objašnjava opseg obrade diljem grada, uključujući treće strane uključene u obradu i njihove uloge.
- Gradovi moraju uspostaviti sustave u skladu s individualnim pravima, osiguravajući da kupljeni proizvodi mogu zadovoljiti te potrebe.
- Gradovi i partneri iz industrije koji zajednički provode projekte trebali bi prije početka obrade zajednički rješavati pitanja upravljanja.

Industrija

- Industrija bi trebala izgraditi sustave koji imaju fleksibilnost za utvrđivanje organizacijskih mjera i donošenje tehničkih mjera kako bi se zadovoljilo ograničenje svrhe.
- Industrija bi trebala osigurati da njihovi proizvodi odražavaju najbolje prakse u industriji, kao što je mogućnost primanja sigurnosnih nadogradnji, provođenja politike otkrivanja ranjivosti i da se ne koriste univerzalne zadane lozinke.
- Gradovi i partneri iz industrije koji zajednički provode projekte trebali bi prije početka obrade zajednički rješavati pitanja upravljanja.

Regulatori

- Regulatorna tijela trebala bi izraditi smjernice o mjerama odgovornosti i upravljačkim strukturama, uključujući smjernice o obradi s više uključenih sudionika.
- Regulatorna tijela trebala bi gradovima i industriji pružiti smjernice o metodama za smanjenje količine podataka, uključujući i sakupljanje.
- Regulatorna tijela trebala bi pružati smislene informacije o pravima građana u vezi s obradom osobnih podataka u inicijativama za pametne gradove.