



Bruxelles, 10.1.2017.  
COM(2017) 9 final

**KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, VIJEĆU,  
EUROPSKOM GOSPODARSKOM I SOCIJALNOM ODBORU I ODBORU REGIJA**

**„STVARANJE EUROPSKOG PODATKOVNOG GOSPODARSTVA”**

{SWD(2017) 2 final}

## „STVARANJE EUROPSKOG PODATKOVNOG GOSPODARSTVA”

### 1. UVOD

Podaci su postali bitan resurs za gospodarski rast, otvaranje novih radnih mjesta i društveni napredak. Analiza podataka omogućuje optimizaciju procesa i odluka, inovacije i predviđanje budućih događaja. Taj globalni trend ima golem potencijal u različitim područjima, od zdravstva, zaštite okoliša, sigurnosti hrane, klime i učinkovitosti resursa do energetike, inteligentnih prometnih sustava i pametnih gradova.

„Podatkovnom gospodarstvu”<sup>1</sup> svojstven je ekosustav različitih vrsta sudionika na tržištu, kao što su proizvođači, istraživači i pružatelji infrastrukture, koji surađuju u cilju osiguravanja dostupnosti i upotrebljivosti podataka. Time se sudionicima na tržištu omogućuje ostvarivanje vrijednosti iz tih podataka stvaranjem različitih aplikacija s velikim potencijalom za poboljšanje svakodnevnog života (npr. upravljanje prometom, optimizacija žetvi ili zdravstvena skrb na daljinu).

U 2014. vrijednost podatkovnoga gospodarstva EU-a procijenjena je na 257 milijardi EUR odnosno 1,85 % BDP-a EU-a<sup>2</sup>. Njegova se vrijednost 2015. povećala na 272 milijarde EUR, odnosno 1,87 % BDP-a EU-a (godišnji rast od 5,6 %). U istoj je procjeni predviđeno da će se, ako se pravovremeno uspostave uvjeti okvira politike i pravnog okvira za podatkovno gospodarstvo, njegova vrijednost do 2020. povećati na 643 milijarde EUR, što će činiti 3,17 % ukupnog BDP-a EU-a.

U skladu s Općom uredbom o zaštiti podataka (Opća uredba)<sup>3</sup> od svibnja 2018. na snagu stupa jedinstveni paneuropski skup pravila kojim će se zamijeniti 28 nacionalnih zakona koji su danas na snazi. Novouspostavljenim mehanizmom „sve na jednom mjestu”<sup>4</sup> osigurat će se da za nadzor prekograničnih postupaka obrade podataka koje provodi poduzeće u EU-u bude odgovorno jedno tijelo za zaštitu podataka. Osigurat će se usklađenost tumačenja novih pravila. Posebno u prekograničnim slučajevima u koje je uključeno nekoliko nacionalnih tijela za zaštitu podataka donijet će se jedinstvena odluka kako bi se osiguralo jednako rješenje za jednake probleme. Nadalje, Općom uredbom uvode se ista pravila za strana poduzeća i poduzeća iz EU-a jer će poduzeća sa sjedištem

---

<sup>1</sup> U podatkovnom gospodarstvu mjere se ukupni učinci tržišta podataka, odnosno tržišta na kojem se digitalni podaci razmjenjuju kao proizvodi ili usluge dobiveni iz neobrađenih podataka, na gospodarstvo kao cjelinu. Ono uključuje generiranje, prikupljanje, pohranu, obradu, distribuciju, analizu, razradu, isporuku i iskorištavanje podataka omogućenih digitalnim tehnologijama (studija europskog tržišta podataka, SMART 2013/0063, IDC, 2016.).

<sup>2</sup> Studija europskog tržišta podataka, SMART 2013/0063, IDC, 2016.

<sup>3</sup> Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/56/EZ (Opća uredba o zaštiti podataka), SL L 119, 4.5.2016., str. 1.

<sup>4</sup> Članak 56. Opće uredbe.

izvan EU-a morati primjenjivati ista pravila kao i europska poduzeća ako pružaju robu i usluge ili prate ponašanje građana na području EU-a. Veća razina povjerenja potrošača bit će od koristi i poslovnim subjektima iz EU-a i onima iz inozemstva.

Direktiva o e-privatnosti odnosi se na povjerljivost elektroničkih komunikacijskih usluga u EU-u. Revizijom Direktive o e-privatnosti, koja se istovremeno s ovom Komunikacijom predlaže u obliku Uredbe<sup>5</sup>, želi se osigurati visoka razina zaštite u potpunosti u skladu s Općom uredbom. Snažnim pravilima o zaštiti podataka stvara se povjerenje na temelju kojeg će se omogućiti razvoj digitalnoga gospodarstva na unutarnjem tržištu.

Kako je predsjednik Juncker naglasio u svojem govoru o stanju Europske unije 14. rujna 2016., *biti Europljanin znači imati pravo na zaštitu svojih osobnih podataka u okviru čvrstih europskih zakona. Jer Europljani ne žele da im bespilotne letjelice nad glavama bilježe svaki korak, a poduzeća svaki klik mišem. Zato su se Parlament, Vijeće i Komisija u svibnju ove godine dogovorili o zajedničkoj europskoj uredbi o zaštiti podataka. Riječ je o čvrstom europskom propisu koji se primjenjuje na sva poduzeća, neovisno o njihovom poslovnom nastanu, svaki put kad ona obrađuju vaše podatke. Jer Europa cijeni privatnost. To je pitanje ljudskog dostojanstva.*

U svojoj Komunikaciji „Zaštita privatnosti u povezanom svijetu – europski okvir za zaštitu podataka za 21. stoljeće”<sup>6</sup> iz 2012. i Komunikaciji „Prema rastućem gospodarstvu temeljenom na podacima”<sup>7</sup> iz 2014. Komisija je prepoznala da su moderna, usklađena pravila diljem EU-a potrebna za slobodan protok podataka iz jedne države članice u drugu, da europsko digitalno gospodarstvo zaostaje u prihvaćanju podatkovne revolucije u usporedbi s SAD-om i da mu nedostaje usporediva industrijska sposobnost. Zaključila je da nepostojanje pravnog okruženja prilagođenog trgovini podacima u EU-u može pridonijeti nedostatku pristupa velikim skupovima podataka, mogućim ulaznim preprekama za nove sudionike na tržištu i gušenju inovacija.

Neopravdanim **ograničenjima slobodnog kretanja podataka** mogao bi se otežati razvoj podatkovnoga gospodarstva EU-a. Ta se ograničenja odnose na zahtjeve koje javna tijela propisuju u vezi s lokacijom podataka u svrhu pohrane i obrade. Pitanje slobodnog kretanja podataka odnosi se na sve vrste podataka: poduzeća i subjekti u podatkovnom gospodarstvu posluju s industrijskim i strojno generiranim podacima, bez obzira na to jesu li ti podaci osobni ili ne, i s podacima nastalima zahvaljujući ljudskom djelovanju. U strategiji jedinstvenog digitalnog tržišta Komisija je najavila da će predložiti inicijativu za rješavanje problema ograničenja slobodnog kretanja podataka na području EU-a zbog razloga koji nisu zaštita osobnih podataka i problema neopravdanih ograničenja povezanih s lokacijom podataka u svrhu pohrane i obrade. Takva ograničenja uključuju pravne akte koje donose države članice te administrativna pravila i prakse s jednakim učinkom. S rastom podatkovnoga gospodarstva njihov se broj povećava, što dovodi do nesigurnosti u pogledu toga gdje se podaci mogu pohranjivati ili obrađivati. To može utjecati na sve sektore gospodarstva te na organizacije privatnog i javnog sektora, koje bi mogle imati poteškoća u pristupu inovativnijim i/ili jeftinijim podatkovnim uslugama.

---

<sup>5</sup> COM (2017) 10

<sup>6</sup> COM (2012) 9

<sup>7</sup> COM (2014) 442

Neopravdanim ograničenjima u pogledu lokacije podataka narušavaju se sloboda pružanja usluga i sloboda poslovnog nastana propisane Ugovorom i njima se krši relevantno sekundarno pravo. To dovodi do rizika od fragmentacije tržišta, smanjenja kvalitete usluga za korisnike i manje konkurentnosti pružatelja podatkovnih usluga, posebno manjih subjekata.

I neopravdana lokalizacija podataka dio je rasprava između EU-a i njegovih trgovinskih partnera s obzirom na sve veću važnost podataka i podatkovnih usluga u globalnom gospodarstvu i potencijalne stavove trećih zemalja o tom pitanju. EU-ova pravila o zaštiti podataka ne smiju biti predmet pregovora u okviru sporazuma o slobodnoj trgovini. Kako je objašnjeno u Komunikaciji o razmjeni i zaštiti osobnih podataka u globaliziranom svijetu<sup>8</sup>, dijalozi o zaštiti podataka i trgovinski pregovori s trećim zemljama moraju se odvijati zasebno. Komisija će osim toga, kako je navedeno u Komunikaciji „Trgovina za sve”<sup>9</sup>, nastojati upotrijebiti sve sporazume o slobodnoj trgovini za uspostavu pravila za e-trgovinu i prekogranične tokove podataka i pozabaviti se novim oblicima digitalnog protekcionizma potpuno u skladu s pravilima EU-a o zaštiti podataka i ne dovodeći ta pravila u pitanje.

Nadalje, kako podatkovna transformacija prodire u gospodarstvo i društvo, strojevi ili procesi koji se temelje na tehnologijama u nastajanju, kao što su internet stvari, tvornice budućnosti i autonomni povezani sustavi, generiraju sve veće količine podataka. Povezanost sama po sebi mijenja način pristupa podacima: podaci kojima se obično pristupalo fizičkim vezama sada su u sve većoj mjeri dostupni na daljinu. Iznimna raznolikost izvora i vrsta podataka i velike mogućnosti primjene uvida u te podatke na različitim područjima, uključujući za razvoj javne politike, tek se pojavljuju. Kako bi i javni i privatni subjekti na podatkovnom tržištu iskoristili te mogućnosti, moraju imati pristup velikim i različitim skupovima podataka. Pitanja pristupa podacima koje generiraju ti strojevi ili procesi i njihova prijenosa stoga su ključna za stvaranje podatkovnog gospodarstva i zahtijevaju pažljivu procjenu.

Druga nova pitanja odnose se na primjenu pravila o odgovornosti za svu štetu prouzročenu kvarom povezanog uređaja ili robota te na prenosivost i interoperabilnost podataka. U kontekstu novih tehnologija kao što su internet stvari ili robotika postoji složena i sofisticirana međuovisnost unutar proizvoda (na temelju hardvera i softvera), ali i među međusobno povezanim uređajima. Štoviše, mogu se pojaviti nova pitanja povezana s autonomnim strojevima, koji svojim neočekivanim i nehotičnom ponašanjem mogu nanijeti štetu osobama i predmetima. Te pojave mogu dovesti do pravne nesigurnosti u pogledu primjene postojećeg okvira za odgovornost i sigurnost.

Kako je najavljeno u strategiji jedinstvenog digitalnog tržišta, cilj je Komisije stvoriti jasan i prilagođen okvir politike i pravni okvir za podatkovno gospodarstvo uklanjanjem preostalih prepreka kretanju podataka i rješavanjem pravnih nesigurnosti koje su posljedica novih podatkovnih tehnologija. Daljnji ciljevi na kojima se temelji ova Komunikacija uključuju povećanje dostupnosti i uporabe podataka, poticanje novih podatkovnih poslovnih modela, poboljšanje uvjeta pristupa podacima i razvoj

---

<sup>8</sup> COM (2017) 7

<sup>9</sup> COM (2015) 497

podatkovne analitike u EU-u. U tu svrhu Komisija predstavlja fokusirana pitanja za raspravu u cilju „stvaranja europskog podatkovnog gospodarstva”.

U skladu s time ovom su Komunikacijom obuhvaćena sljedeća pitanja: slobodan protok podataka, pristup i prijenos strojno generiranih podataka, odgovornost i sigurnost u kontekstu tehnologija u nastajanju te prenosivost neosobnih podataka, interoperabilnost i standardi. Ovom se Komunikacijom utvrđuju i prijedlozi za testiranje zajedničkih regulativnih rješenja u stvarnom okruženju.

Komisija pokreće sveobuhvatan dijalog s dionicima o pitanjima koja se razmatraju u ovoj Komunikaciji. Prva je faza tog dijaloga javno savjetovanje, objavljeno paralelno s paketom o podatkovnom gospodarstvu<sup>10</sup>.

## 2. SLOBODAN PROTOK PODATAKA

Za dinamično podatkovno gospodarstvo koje dobro funkcionira potrebno je omogućiti i zaštititi protok podataka na unutarnjem tržištu. U kontekstu brzog razvoja tehnologije siguran i pouzdan slobodan protok podataka ključan je za zaštitu četiriju temeljnih sloboda jedinstvenog tržišta EU-a utvrđenih u Ugovorima (roba, radnici, pružanje usluga i kapital). Podatkovne usluge brzo rastu u EU-u i svijetu. Učinkovitim jedinstvenim tržištem bez prepreka u tom sektoru stvorile bi se znatne prilike za dodatan rast i otvaranje novih radnih mjesta.

Taj rast i inovacije u podatkovnom gospodarstvu te provedba prekograničnih javnih usluga mogu se ugroziti preprekama slobodnom kretanju podataka u EU-u, kao što su neopravdani zahtjevi u pogledu lokalizacije podataka koje propisuju javna tijela. Mjerama za lokalizaciju podataka zapravo se ponovno uvode digitalne „kontrole granica”<sup>11</sup>. One među ostalim obuhvaćaju zahtjeve nadzornih tijela da pružatelji financijskih usluga svoje podatke pohranjuju lokalno, provedbu pravila o poslovnoj tajni koja podrazumijevaju lokalnu pohranu ili obradu podataka i opsežne propise kojima se zahtijeva lokalna pohrana arhiviranih informacija koje generira javni sektor bez obzira na njihovu osjetljivost.

Zabrinutost zbog privatnosti opravdana je, ali je javna tijela ne bi trebala upotrebljavati kao razlog za neopravdano ograničenje slobodnog protoka podataka. Kako je već navedeno, Općom uredbom uvodi se jedinstveni skup pravila s visokom razinom zaštite osobnih podataka u cijelom EU-u. Njome se jača povjerenje potrošača u internetske usluge i osigurava jedinstvena primjena pravila u svim državama članicama preko snažnijih nacionalnih tijela za zaštitu podataka. Općom uredbom potiče se stvaranje povjerenja potrebnog za obradu podataka i ona čini temelj slobodnog protoka osobnih podataka u EU-u. Njome se uklanjaju ograničenja slobodnog kretanja osobnih podataka unutar Unije koja se temelje na razlozima povezanim sa zaštitom osobnih podataka<sup>12</sup>.

---

<sup>10</sup> <https://ec.europa.eu/digital-single-market/news-redirect/52039>

<sup>11</sup> OECD, *Emerging Policy Issues: Localisation Barriers to Trade* („Nova pitanja politike: trgovinske prepreke povezane s lokalizacijom”), 2015. i tekući rad.

<sup>12</sup> Članak 1. stavak 3. Npr. dinamična IP adresa koju pružatelj internetskih medijskih usluga registrira kada osoba pristupa web-mjestu koje taj pružatelj čini dostupnim javnosti smatra se, u pogledu dotičnog pružatelja, osobnim podatkom ako raspolaze pravnim sredstvima koja mu omogućuju da utvrdi dotičnu osobu na temelju dodatnih

Međutim, ograničenja koja se temelje na razlozima koji nisu zaštita osobnih podataka, npr. ona u skladu s poreznim ili računovodstvenim propisima, nisu obuhvaćena Općom uredbom. Nadalje, neosobni podaci, tj. podaci koji nisu povezani s fizičkom osobom čiji je identitet utvrđen ili se može utvrditi<sup>13</sup>, i dalje su izvan područja primjene Opće uredbe. To, primjerice, mogu biti neosobni strojno generirani podaci.

Ograničenja povezana s lokalizacijom podataka mogu biti posljedica pravnih propisa ili upravnih smjernica ili prakse kojima se zahtijeva da pohranjivanje ili obrada podataka<sup>14</sup> u elektroničkom formatu<sup>15</sup> budu ograničeni na određeno zemljopisno područje ili jurisdikciju. Ponekad ograničenja uvode države članice jer smatraju da nadzorna tijela mogu lakše nadzirati lokalno pohranjene podatke. Lokalizacija služi i kao zamjena za jamstva u pogledu privatnosti, revizije, izvršenja zakonodavstva i sigurnosti podataka. Međutim, u praksi se tim mjerama rijetko pridonosi ciljevima koji se njima žele ostvariti.

Osim o fizičkoj lokaciji na kojoj su podaci pohranjeni, informacijska sigurnost ovisi o nizu čimbenika kao što su čuvanje povjerljivosti i integriteta podataka ako su stavljeni na raspolaganje izvan objekta u kojem su pohranjeni. U tom pogledu, ono što uistinu omogućuje sigurnu pohranu i obradu podataka nisu ograničenja povezana s lokacijom podataka, već najnovije dobre prakse u upravljanju informacijskim i komunikacijskim tehnologijama primijenjene u razmjerima daleko većima od pojedinačnih sustava. Na primjer, da bi se podaci zaštitili u slučaju lokalnih prirodnih katastrofa ili kibernetičkih napada, objekti za pohranu podataka koji se nalaze u različitim državama članicama mogli bi se međusobno podupirati te bi mogli iskoristiti tehničke i organizacijske mjere propisane Direktivom o sigurnosti mrežnih i informacijskih sustava<sup>16</sup>. Štoviše, dostupnost podataka za regulativne ili nadzorne potrebe, koja se ni u kojem slučaju ne dovodi u pitanje, bolje bi se osigurala jačanjem suradnje među nacionalnim tijelima ili između tih tijela i privatnog sektora umjesto ograničenjima povezanim s lokalizacijom. Ta bi ograničenja mogla imati upravo suprotan učinak u područjima za koja je znakovita bliska suradnja nadzornih tijela, primjerice u području financijskih usluga<sup>17</sup>.

Neovisno o tome, zahtjevi u pogledu lokalizacije podataka mogu biti opravdani i proporcionalni u određenim kontekstima ili u vezi s određenim podacima, posebno prije uspostave učinkovitih mehanizama prekogranične suradnje, kao što su osiguravanje sigurnog tretmana određenih podataka koji se odnose na ključnu energetsku

---

informacija koje pružatelj internetske usluge ima o toj osobi. Vidi presudu u predmetu C-582/14, Breyer, ECLI:EU:C:2016:779, točku 49.

<sup>13</sup> Kako je definirano u članku 4. stavku 1. Opće uredbe.

<sup>14</sup> Podaci i u privatnom i u javnom vlasništvu.

<sup>15</sup> Uključujući kopije skupova podataka.

<sup>16</sup> Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, SL L 194, 19.7.2016., str. 1–30.

<sup>17</sup> Izvjesnim brojem odredaba EU-a o financijskim uslugama i Europskim sustavom financijskog nadzora zahtijeva se da nadzorna tijela imaju pristup podacima o financijskim institucijama i transakcijama bilo gdje na području EU-a. Zahtjevima za pohranu podataka na određenom državnom području ili zahtjevima kojima se pristup u svrhu nadzora uvjetuje administrativnim postupcima mogao bi se ograničiti pristup nadzornih tijela podacima koji su im bitni za provedbu svojih ovlasti.

infrastrukturu, dostupnost elektroničkih dokaza (npr. kao lokaliziranih kopija skupova podataka) za tijela za izvršavanje zakonodavstva ili lokalna pohrana podataka koji se čuvaju u određenim javnim registrima.

Nažalost, u svijetu i Europi raste trend lokalizacije podataka, što je pristup koji se često temelji na pogrešnoj predodžbi da su lokalizirane usluge automatski sigurnije od prekograničnih usluga. Štoviše, na tržište podatkovnih usluga znatno utječe nedostatak transparentnih pravila i snažna percepcija potrebe za lokalizacijom podataka. Time se poduzećima i organizacijama javnog sektora može ograničiti pristup jeftinijim ili inovativnijim podatkovnim uslugama ili prisiliti poduzeća koja posluju prekogranično na ugovaranje kapaciteta za pohranu i obradu viška podataka. Nadalje, time bi se poduzeća čija se djelatnost temelji na podacima, posebno novoosnovana poduzeća i MSP-ove, moglo spriječiti da prošire svoje djelatnosti, uđu na nova tržišta (npr. zbog toga što moraju uložiti u podatkovne centre u 28 država članica) ili centraliziraju podatkovne i analitičke kapacitete u svrhu razvoja novih proizvoda i usluga.

Europa trenutačno interno odnosno unutar EU-a zadovoljava 84 % svoje krajnje potražnje za uslugama „povezanim s IKT-om” (savjetovanje, smještaj na poslužitelju, razvoj). Kada bi se zahvaljujući uklanjanju ograničenja u pogledu lokalizacije podataka te usluge mogle lakše pružati prekogranično unutar EU-a, BDP bi se zbog manjih troškova i veće učinkovitosti mogao povećati za do 8 milijardi EUR godišnje<sup>18</sup>.

Lokalizacija podataka onemogućuje i šire korištenje usluga pohrane i računalstva u oblaku. To može imati i šire društvene posljedice. Učinkovitijom uporabom informatičkih resursa moglo bi se pridonijeti neto smanjenju potrošnje energije i emisija ugljika za najmanje 30 %. Malo poduzeće koje prijeđe na poslovanje u oblaku moglo bi smanjiti svoju potrošnju energije i emisije ugljika za više od 90 % tako da se za rad svojih poslovnih aplikacija služi oblakom umjesto vlastitom infrastrukturom. Očekuje se da će se do kraja 2020. globalno tržište energetske učinkovitih podatkovnih centara povećati na gotovo 90 milijardi EUR. Fragmentiranim tržištem podatkovnih usluga spriječio bi se potpuni razvoj tih energetske učinkovitih usluga u EU-u i dovela bi se u opasnost i spremnost na ulaganje.

Kako bi se riješila navedena pitanja i uklonila navedena ograničenja te ostvario puni potencijal europskog podatkovnog gospodarstva, sva djelovanja svih država članica koja utječu na pohranu ili obradu podataka trebala bi se voditi „**načelom slobodnog kretanja podataka unutar EU-a**” koje proizlazi iz njihovih obveza na temelju odredaba o slobodnom kretanju usluga i slobodnom nastanu iz Ugovora i relevantnog sekundarnog zakonodavstva. Sva postojeća ili nova ograničenja u pogledu lokacije podataka trebala bi biti pažljivo opravdana na temelju Ugovora i relevantnog sekundarnog zakonodavstva kako bi se provjerilo jesu li potrebna i proporcionalna za postizanje prevladavajućeg cilja od općeg interesa, kao što je javna sigurnost<sup>19</sup>.

---

<sup>18</sup> *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States*, („Oslobađanje unutarnjih tokova podataka u EU-u: ekonomska procjena mjera za lokalizaciju podataka u državama članicama EU-a”), ECIPE, 2016., izračun na temelju povećanog konkurentskog pritiska u okviru u potpunosti cjenovno transparentnog „industrijskog” jedinstvenog digitalnog tržišta.

<sup>19</sup> Uzimajući u obzir činjenicu da izuzeća od Ugovora treba tumačiti restriktivno. Takvo relevantno sekundarno zakonodavstvo uključuje Opću uredbu, Direktivu 2000/31/EZ (Direktiva o e-trgovini), Direktivu 2006/123/EZ (Direktiva o uslugama) i, u pogledu nacrtu tehničkih propisa i nacrtu pravila o uslugama informacijskog društva, Direktivu 2015/1535 (Direktiva o transparentnosti).

Načelo slobodnog kretanja osobnih podataka<sup>20</sup> utvrđeno u primarnom i sekundarnom zakonodavstvu trebalo bi se primjenjivati i u slučajevima u kojima se Općom uredbom državama članicama dopušta reguliranje određenih pitanja. Države članice trebalo bi poticati da uvodne izjave iz Opće uredbe ne upotrebljavaju za daljnje ograničavanje slobodnog protoka podataka.

Europsko vijeće je u svojim zaključcima od 15. prosinca 2016. pozvalo na uklanjanje preostalih prepreka u okviru jedinstvenog tržišta, uključujući one koje ometaju slobodan protok podataka<sup>21</sup>.

Za provedbu načela slobodnog kretanja podataka Komisija će poduzeti sljedeća dva koraka:

- nakon objave ove Komunikacija Komisija će s državama članicama i ostalim dionicima započeti strukturirane dijaloge o opravdanjima za mjere povezane s lokacijom podataka i o njihovoj proporcionalnosti, uzimajući kao polazište ograničenja koja je Komisija utvrdila do sada.
- Komisija će na temelju ishoda dijaloga i daljnjeg prikupljanja dokaza o razmjerima i prirodi ograničenja u pogledu lokacije podataka i njihovih učinaka, prije svega na MSP-ove i novoosnovana poduzeća, među ostalim i u okviru popratnog javnog savjetovanja, po potrebi pokrenuti postupak u slučaju povrede prava kako bi uklonila neopravdana ili neproporcionalna ograničenja u pogledu lokacije podataka i može, bude li to potrebno, donijeti dodatne inicijative o slobodnom protoku podataka. U tom će se kontekstu svako daljnje djelovanje poduzeti u skladu s načelima bolje regulative.

### 3. PRISTUP PODACIMA I NJIHOV PRIJENOS

Strojevi ili procesi koji se temelje na tehnologijama u nastajanju, kao što je internet stvari, generiraju sve veće količine podataka. Takvi se podaci sve češće upotrebljavaju kao ključna komponenta novih i inovativnih usluga radi poboljšanja proizvoda ili proizvodnog procesa i pružanja podrške pri odlučivanju.

Za sudionike na podatkovnom tržištu raznolikost podataka koje generiraju ti strojevi ili procesi predstavlja mnoštvo prilika za inovacije i primjenu uvida stečenih na temelju tih podataka. Na primjer, podaci prikupljeni senzorima koji se upotrebljavaju na modernim poljoprivrednim gospodarstvima mogli bi se upotrijebiti za stvaranje aplikacije za optimizaciju žetve ili bi se podaci koje generiraju senzori u semaforima mogli upotrijebiti za stvaranje aplikacije za upravljanje prometom ili optimizaciju puta.

<sup>20</sup> Slobodno kretanje osobnih podataka utvrđeno je u članku 16. Ugovora o funkcioniranju Europske unije, dok se pravila o slobodnom kretanju osobnih podataka utvrđuju postojećim i budućim zakonodavstvom EU-a o zaštiti podataka. U članku 1. stavku 3. Opće uredbe o zaštiti podataka navodi se sljedeće: „Slobodno kretanje osobnih podataka unutar Unije ne ograničava se niti se zabranjuje iz razloga povezanih sa zaštitom pojedinaca u pogledu obrade osobnih podataka”.

<sup>21</sup> <http://www.consilium.europa.eu/eu/en/press-releases/2016/12/15-euro-conclusions-final/>

Kako bi se ostvarila maksimalna vrijednost iz takve vrste podataka, sudionici na tržištu trebaju imati pristup velikim i različitim skupovima podataka. Međutim, to je teško postići ako subjekti koji generiraju podatke zadržavaju te podatke za sebe i ako se podaci posljedično analiziraju u izoliranim sustavima. Pitanja pristupa i prijenosa povezana s neobrađenim podacima (podaci koji nisu obrađeni ili izmijenjeni od bilježenja) koje generiraju ti strojevi ili procesi stoga su ključna za stvaranje podatkovnoga gospodarstva i zahtijevaju pažljivu procjenu.

Pitanje pristupa strojno generiranim podacima razmatra se u nekoliko sektora, kao što su promet, energetska tržišta, pametno životno okruženje, zdravstveni sektor i sektor skrbi.

Prije ispitivanja trenutačne situacije u pogledu pristupa podacima u EU-u važno je objasniti o kojoj je vrsti podataka riječ u ovom kontekstu.

### **3.1. Vrsta podataka**

Podaci općenito mogu biti osobni ili neosobni. Na primjer, podaci koje generiraju kućni toplinski senzori mogu po svojoj prirodi biti osobni ako se mogu povezati sa živom osobom, dok podaci o vlažnosti tla nisu osobni. Osobni podaci mogu se pretvoriti u neosobne postupkom anonimizacije. Ako je riječ o podacima koji se smatraju osobnim podacima<sup>22</sup>, primjenjuje se okvir za zaštitu podataka, posebno Opća uredba.

Strojno generirani podaci nastaju u računalnim procesima, aplikacijama ili uslugama bez izravne ljudske intervencije ili ih proizvode senzori koji obrađuju informacije primljene od opreme, softvera ili strojeva bilo virtualno ili stvarno.

Strojno generirani podaci mogu po prirodi biti osobni ili neosobni. Ako strojno generirani podaci omogućuju utvrđivanje identiteta fizičke osobe, smatraju se osobnim podacima, a to podrazumijeva da se sva pravila o osobnim podacima primjenjuju sve dok ti podaci ne budu u potpunosti anonimizirani (npr. podaci o lokaciji iz mobilnih aplikacija).

Poveznica između slobodnog protoka podataka i novih pitanja pristupa podacima i njihova prijenosa jest činjenica da će poduzeća i subjekti u podatkovnom gospodarstvu obrađivati i osobne i neosobne podatke i da će tokovi i skupovi podataka redovito sadržavati obje vrste podataka. U svim mjerama politike moraju se uzeti u obzir ta gospodarska stvarnost i pravni okvir za zaštitu osobnih podataka uz istodobno poštovanje temeljnih prava pojedinaca.

### **3.2. Ograničen pristup podacima**

Za procjenu tog novog pitanja treba prvo analizirati kako poduzeća i ostali sudionici na tržištu mogu pristupiti velikim i različitim skupovima podataka koji su potrebni u podatkovnom gospodarstvu.

---

<sup>22</sup> Kako je definirano u članku 4. stavku 1. Opće uredbе.

Raspoloživi dokazi<sup>23</sup> upućuju na to da poduzeća koja raspolažu velikim količinama podataka općenito upotrebljavaju uglavnom vlastite kapacitete za podatkovnu analitiku. U većini slučajeva podatke generira i analizira isto poduzeće, a čak i kada je analiza podataka povjerena podugovornoj strani, daljnja ponovna uporaba podataka nije moguća. Nadalje, u nekim slučajevima proizvođači, poduzeća koja pružaju usluge ili drugi sudionici na tržištu koji posjeduju podatke zadržavaju za sebe podatke koje generiraju njihovi strojevi ili koji su generirani njihovim proizvodima i uslugama te tako potencijalno ograničavaju ponovnu uporabu na podređenim tržištima. Mnoga poduzeća ne iskorištavaju ili korisnicima ne omogućuju pristupačna sučelja za programiranje aplikacija (API-jevi)<sup>24</sup> (kojima se utvrđuje kako bi različite aplikacije trebale međusobno funkcionirati) koja mogu služiti kao sigurne ulazne točke za nove i inovativne uporabe podataka u vlasništvu poduzeća.

Stoga je razmjena podataka općenito i dalje ograničena. Tržišta podataka polako nastaju, ali njihova uporaba nije proširena. Poduzeća možda ne raspolažu pravim alatima i vještinama za kvantifikaciju gospodarske vrijednosti svojih podataka i možda se boje gubitka ili ugrožavanja svoje konkurentске prednosti ako podaci postanu dostupni konkurentima.

### **3.3. Neobrađeni strojno generirani podaci: pravna situacija na razini EU-a i nacionalnoj razini**

Neobrađeni strojno generirani podaci nisu zaštićeni postojećim pravima intelektualnog vlasništva jer se smatra da nisu rezultat intelektualnog napora i/ili da nemaju nikakav stupanj originalnosti. U skladu s pravom *sui generis* iz Direktive o bazama podataka (96/9/EZ), kojim se proizvođačima baza podataka daje pravo sprječavanja izvlačenja i/ili ponovne uporabe cijele baze podataka ili znatnog dijela sadržaja baze podataka, zaštita se može osigurati samo pod uvjetom da stvaranje takve baze podataka uključuje znatno ulaganje u postizanje, verifikaciju ili predstavljanje njezina sadržaja. Nedavno donesenom Direktivom o zaštiti poslovnih tajni (2016/943/EU), koja se mora prenijeti u nacionalno pravo do lipnja 2018., osigurat će se zaštita poslovnih tajni od nezakonitog pribavljanja, korištenja i otkrivanja. Kako bi se podaci smatrali „poslovnom tajnom”, moraju se poduzeti mjere za zaštitu tajnosti informacija koje predstavljaju „intelektualni kapital poduzeća”.

Na podatke se u skladu s pravom različitih država članica primjenjuju pravni zahtjevi samo ako ti podaci ispunjuju posebne uvjete na temelju kojih ih se može smatrati, na primjer, pravom intelektualnog vlasništva, pravom baza podataka ili poslovnom tajnom. Međutim, na razini EU-a neobrađeni strojno generirani podaci kao takvi općenito ne bi ispunili relevantne uvjete.

Stoga na nacionalnoj razini ili razini Unije trenutačno ne postoje sveobuhvatni okviri politike za neobrađene strojno generirane podatke koji se ne smatraju osobnim podacima

---

23 IDC, Studija europskog tržišta podataka, Prvo privremeno izvješće, 2016.; Popratna studija procjene učinka u području novih pitanja vlasništva podataka, interoperabilnosti, (ponovne) uporabe i pristupa podacima te odgovornosti, Prvo privremeno izvješće, 2016.; konferencija na visokoj razini Glavne uprave za komunikacijske mreže, sadržaje i tehnologije, 17. listopada 2016.

24 Na primjer: <https://developer.lufthansa.com/>, <https://data.sncf.com/api>, <https://api.tfl.gov.uk/>; <https://dev.blablacar.com/>

ili za uvjete njihova ekonomskog iskorištavanja i utrživosti. To se pitanje najčešće uređuje ugovornim rješenjima. Dostatan odgovor mogla bi biti upotreba postojećih instrumenata općeg ugovornog prava i prava tržišnog natjecanja koji su dostupni u Uniji. Osim toga, mogli bi se predvidjeti dobrovoljni ili krovni sporazumi koji bi obuhvaćali određene sektore. Neovisno o tome, ako različiti sudionici na tržištu nemaju jednaku pregovaračku moć, tržišna rješenja sama po sebi možda neće biti dostatna za osiguranje pravednih rezultata kojima se pogoduje inovacijama, omogućivanje jednostavnog pristupa za nove sudionike na tržištu i izbjegavanje ovisnosti.

### 3.4. Situacija u praksi

U određenim slučajevima proizvođači ili pružatelji usluga mogu postati *de facto* „vlasnici” podataka koje generiraju njihovi strojevi ili procesi, čak i ako su ti strojevi u vlasništvu korisnika. *De facto* kontrola tih podataka može biti izvor diferencijacije i konkurentske prednosti za proizvođače. Međutim, to može biti problematično jer proizvođač često sprječava korisnika da drugoj strani odobri uporabu podataka.

Različiti sudionici na tržištu koji kontroliraju podatke stoga mogu, ovisno o posebnostima tržišta, iskoristiti nedostatke u regulativnom okviru ili prethodno opisane pravne nesigurnosti na način da korisniku nametnu nepoštene standardne uvjete ugovora ili uporabom tehničkih sredstava, kao što su vlasnički format ili enkripcija. Iako je nekoliko država članica proširilo područje primjene Direktive o nepoštenim uvjetima ugovora u području zaštite potrošača i na transakcije među poduzećima (B2B), to nisu učinile sve države članice. To bi moglo dovesti do toga da, primjerice, korisnici i poduzeća u sve većoj mjeri budu vezani isključivim dogovorima o iskorištavanju podataka. Mogla bi se pojaviti praksa dobrovoljnog dijeljenja podataka, ali bi pregovori o takvim ugovorima mogli podrazumijevati znatne transakcijske troškove za slabije stranke u slučaju nejednakog pregovaračkog položaja ili znatnih troškova najma stručne pravne pomoći.

### 3.5. Budući okvir EU-za pristup podacima

Mogućnost osiguravanja pristupa strojno generiranim podacima trenutačno ispituje nekoliko država članica, koje mogu odlučiti same urediti to pitanje. Neusklađeni pristup mogao bi dovesti do fragmentacije i bio bi štetan za razvoj podatkovnoga gospodarstva EU-a te funkcioniranje prekograničnih podatkovnih usluga i tehnologija na unutarnjem tržištu.

Komisija se stoga namjerava uključiti u dijalog s državama članicama i ostalim dionicima kako bi razmotrila mogući budući okvir EU-a za pristup podacima. Prema mišljenju Komisije u tom bi se dijalogu trebalo usredotočiti na najučinkovitije načine postizanja sljedećih ciljeva:

- **poboljšanje pristupa anonimnim strojno generiranim podacima:** dijeljenjem, ponovnom uporabom i objedinjavanjem strojno generirani podaci postaju izvor stvaranja vrijednosti, inovacija i raznolikosti poslovnih modela<sup>25</sup>

---

<sup>25</sup> Ako je riječ o osobnim podacima, primjenjuje se Opća uredba.

- **olakšavanje i poticanje dijeljenja takvih podataka:** svakim budućim rješenjem trebalo bi njegovati učinkovit pristup podacima, uzimajući u obzir, na primjer, moguće razlike u pregovaračkoj moći sudionika na tržištu
- **zaštitu ulaganja i imovine:** u svakom budućem rješenju trebalo bi uzeti u obzir i legitimne interese sudionika na tržištu koji ulažu u razvoj proizvoda, osigurati im pravedan povrat ulaganja i time pridonijeti inovacijama. Istovremeno, svakim budućim rješenjem trebala bi se osigurati pravedna raspodjela koristi među imateljima podataka<sup>26</sup>, izvršiteljima obrade i pružateljima aplikacija u vrijednosnim lancima;
- **izbjegavanje otkrivanja povjerljivih podataka:** svakim budućim rješenjem trebalo bi ublažiti rizik otkrivanja povjerljivih podataka, posebno postojećim ili potencijalnim konkurentima. U tom bi pogledu trebalo omogućiti i pravilnu klasifikaciju podataka prije procjene može li se određeni podatak dijeliti ili ne;
- **maksimalno smanjenje učinaka ovisnosti:** trebalo bi uzeti u obzir nejednaku pregovaračku moć poduzeća i privatnih osoba. Trebalo bi izbjegavati situacije ovisnosti, posebno u slučaju MSP-ova, novoosnovanih poduzeća i privatnih osoba.

U dijalozima s dionicima Komisija namjerava raspraviti o sljedećim mogućnostima za rješavanje pitanja pristupa strojno generiranim podacima, koje se razlikuju s obzirom na razinu intervencije:

- **smjernice za poticanje poduzeća na dijeljenje podataka:** kako bi ublažila učinke različitih nacionalnih propisa i osigurala veću pravnu sigurnost za poduzeća, Komisija bi mogla izdati smjernice o tome kako bi u ugovorima trebalo riješiti prava kontrole neosobnih podataka. Te bi se smjernice temeljile na postojećem zakonodavstvu, posebno na zahtjevima transparentnosti i pravednosti utvrđenima tržišnim i potrošačkim pravom EU-a, Direktivom o poslovnim tajnama i zakonodavstvom o autorskim pravima, posebno Direktivom o bazama podataka. Komisija planira evaluaciju Direktive o bazama podataka u 2017.;
- **poticanje razvoja tehničkih rješenja za pouzdanu identifikaciju i razmjenu podataka:** sljedivost i jasna identifikacija izvora podataka preduvjet su stvarne kontrole podataka na tržištu. Za stvaranje povjerenja u sustav može biti potrebno definirati pouzdane i po mogućnosti standardizirane protokole za dosljednu identifikaciju izvora podataka. I sučeljima za programiranje aplikacija (API) može se potaknuti stvaranje ekosustava programera aplikacija i algoritama koji su zainteresirani za podatke kojima raspolažu poduzeća. API-jevima se poduzećima i javnim tijelima može pomoći da utvrde različite vrste ponovne uporabe podataka kojima raspolažu i ostvare dobit od njih. Na toj bi se osnovi u okviru tehničkih smjernica mogla razmotriti šira primjena otvorenih, standardiziranih i dobro dokumentiranih API-jeva, uključujući utvrđivanje i širenje najboljih praksi za poduzeća i tijela javnog sektora. To bi moglo uključivati stavljanje podataka na raspolaganje u strojno čitljivim formatima i pružanje povezanih metapodataka;

---

<sup>26</sup> Subjekt koji u praksi upravlja strojno generiranim podacima i zadržava takve podatke.

- **zadana ugovorna pravila:** zadanim pravilima moglo bi se opisati referentno uravnoteženo rješenje za ugovore koji se odnose na podatke, uzimajući pritom u obzir i provjeru prikladnosti cjelokupnog funkcioniranja Direktive o nepoštenim uvjetima ugovora koja je u tijeku. Ona bi se mogla povezati s uvođenjem kontrole nepoštenosti u ugovornim odnosima među poduzećima<sup>27</sup>, što bi za posljedicu imalo poništenje ugovornih klauzula koje prekomjerno odstupaju od zadanih pravila. Moglo bi ih se dopuniti i skupom preporučenih standardnih uvjeta ugovora koje su utvrdili dionici. Takvim bi se pristupom smanjile pravne prepreke za mala poduzeća i umanjila neravnoteža u pregovaračkim položajima te istodobno omogućio viši stupanj slobode ugovaranja;
- **pristup u svrhe javnog interesa i znanstvene svrhe:** javnim tijelima mogao bi se odobriti pristup podacima ako bi to bilo od „općeg interesa” i ako bi se time znatno poboljšalo funkcioniranje javnog sektora, na primjer pristup poslovnim podacima za statističke urede ili optimizacija sustava upravljanja prometom na temelju podataka iz privatnih vozila u stvarnom vremenu. Pristup statističkih tijela poslovnim podacima općenito bi pridonio rasterećivanju gospodarskih subjekata u pogledu statističkog izvješćivanja. Slično tome, pristup podacima iz različitih izvora i mogućnost njihova kombiniranja ključni su za znanstvena istraživanja u područjima kao što su medicinske i društvene znanosti te znanosti o okolišu;
- **prava proizvođača podataka:** pravo uporabe i odobrenja uporabe neosobnih podataka moglo bi se dodijeliti „proizvođaču podatka”, odnosno vlasniku ili dugoročnom korisniku (odnosno zakupcu) uređaja. Cilj tog pristupa bio bi pojasniti pravnu situaciju i ponuditi veći izbor proizvođaču podataka tako da se korisnicima omogući iskorištavanje vlastitih podataka, čime bi pridonijeli oslobađanju strojno generiranih podataka. Međutim, bilo bi potrebno jasno utvrditi relevantna izuzeća, posebno osiguravanje neisključivog pristupa podacima za proizvođača ili javna tijela, na primjer zbog razloga upravljanja prometom ili razloga povezanih s okolišem. Kada je riječ o osobnim podacima, pojedinac će zadržati pravo povlačenja svoje privole u bilo kojem trenutku nakon odobrenja uporabe. Bilo bi potrebno anonimizirati osobne podatke prije nego što se drugoj stranci odobri daljnja uporaba tako da se identitet pojedinca ne može ili više ne može utvrditi. Opća uredba i dalje se primjenjuje na sve osobne podatke (bez obzira na to jesu li generirani strojno ili drukčije) sve do njihove anonimizacije;
- **pristup uz naknadu:** za vlasnike podataka, primjerice proizvođače, pružatelje usluga ili druge stranke, mogao bi se razviti okvir koji bi se mogao temeljiti na određenim ključnim načelima, kao što su poštenu, razumni i nediskriminirajući (FRAND) uvjeti, kako bi se nakon anonimizacije i uz naknadu omogućio pristup podacima kojima oni raspolažu. U obzir bi trebalo uzeti relevantne legitimne interese i potrebu za zaštitom poslovnih tajni. Moglo bi se predvidjeti i uvođenje različitih načina pristupa za različite sektore i/ili poslovne modele kako bi se uzele u obzir posebnosti svake industrije. Na primjer, u pojedinim bi slučajevima

---

<sup>27</sup>. Jasno je da bi se referentna vrijednost za razinu nepoštenosti za ugovore među poduzećima trebala razlikovati od one za ugovore između poduzeća i potrošača kako bi se odrazio viši stupanj slobode ugovaranja u odnosima među poduzećima.

otvoreni pristup podacima (u potpunosti ili djelomično) mogao biti najprimjereniji izbor i za poduzeća i za društvo.

Komisija će se o prethodno navedenim pitanjima savjetovati s dionicima kako bi prikupila što više dokaza o funkcioniranju tržišta podataka po sektorima i istražila moguća rješenja. U tom je kontekstu nužna široka rasprava na makrorazini kako bi se raspravilo o mogućim rješenjima i izbjegle nehotične nuspojave kojima bi se gušile inovacije i narušilo tržišno natjecanje. Osim toga, održat će se posebne sektorske rasprave s relevantnim dionicima u podatkovnom vrijednosnom lancu.

#### **4. ODGOVORNOST**

Još jedno novo pitanje jest i primjena postojećih pravila o odgovornosti u podatkovnom gospodarstvu u vezi s proizvodima i uslugama koji se temelje na tehnologijama u nastajanju kao što su internet stvari, tvornice budućnosti i autonomni povezani sustavi. Internet stvari brzorastuća je mreža svakodnevnih predmeta, kao što su satovi, vozila i termostati, koji su povezani s internetom. Autonomni povezani sustavi, kao što su vozila bez vozača, djeluju neovisno od ljudi te mogu razumjeti i tumačiti svoje okruženje. Te tehnologije u nastajanju služe se senzorima za pružanje različitih vrsta podataka koji su često potrebni za funkcioniranje proizvoda ili usluge.

Svim se tim inovacijama može pridonijeti sigurnijem i kvalitetnijem životu, međutim, za svaki uređaj neizbježno postoji mogućnost konstrukcijskih pogrešaka, nepravilnog rada ili manipulacije. To bi moglo biti posljedica prijenosa pogrešnih podataka senzorom, primjerice, zbog kvara softvera, problema u povezivanju ili neispravnog rada stroja. Zbog prirode tih sustava može biti teško utvrditi točan izvor problema zbog kojeg je šteta nastala, čime se otvara pitanje kako osigurati da ti sustavi budu sigurni za korisnike kako bi se u najvećoj mogućoj mjeri smanjila mogućnost nastanka štete i tko bi trebao biti odgovoran za štetu u slučaju njezina nastanka.

Pitanje kako zajamčiti sigurnost i korisnicima i proizvođačima tih uređaja u pogledu njihove potencijalne odgovornosti stoga je od ključne važnosti za stvaranje podatkovnoga gospodarstva.

##### **4.1. Pravila EU-a o odgovornosti**

U građanskom pravu općenito se razlikuju dvije vrste zakonske odgovornosti: ugovorna, gdje odgovornost za štetu proizlazi iz ugovornog odnosa između stranaka, i izvanugovorna<sup>28</sup>, gdje su odgovornosti utvrđene izvan ugovora. Važna vrsta izvanugovorne odgovornosti jest odgovornost za neispravne proizvode. Na razini EU-a Direktivom o odgovornosti za neispravne proizvode (85/374/EEZ) („Direktiva o odgovornosti za proizvode”) utvrđeno je načelo objektivne odgovornosti, odnosno odgovornosti bez krivnje: ako se zbog neispravnog proizvoda nanese šteta potrošaču, proizvođači mogu biti odgovorni čak i ako nije riječ o nemaru ili krivnji s njihove strane.

---

<sup>28</sup> Pravila EU-a o odgovornosti odnose se samo na izvanugovorne odgovornosti.

No moglo bi postati teško ili nejasno kako primjenjivati odredbe te Direktive<sup>29</sup> u kontekstu interneta stvari i autonomnih povezanih sustava (npr. robotike) zbog sljedećih razloga: svojstva tih sustava, na primjer u slučaju kompliciranog vrijednosnog lanca proizvoda ili usluge, s međuovisnostima između dobavljača, proizvođača i ostalih trećih osoba, nesigurnosti u pogledu pravne prirode uređaja interneta stvari, odnosno jesu li oni proizvodi, usluge ili proizvodi koji dolaze uz prodaju usluge i autonomne prirode tih tehnologija.

Komisija je pokrenula sveobuhvatnu evaluaciju Direktive o odgovornosti za proizvode kako bi procijenila njezino opće funkcioniranje i jesu li njezina pravila, koja su utvrđena za veoma drukčije okruženje, i dalje prikladna za tehnologije u nastajanju kao što su internet stvari i autonomni povezani sustavi.

#### 4.2. Mogući daljnji koraci

Cilj je Komisije povećati pravnu sigurnost u pogledu odgovornosti u kontekstu tehnologija u nastajanju i time stvoriti povoljne uvjete za inovacije. Osim zadržavanja postojećeg stanja<sup>30</sup>, mogli bi se istražiti različiti pristupi, uključujući:

- **pristupe koji se temelje na nastanku rizika ili upravljanju rizicima:** na temelju tih pristupa odgovornost bi se mogla dodijeliti sudionicima na tržištu koji stvaraju velik rizik za ostale ili onim sudionicima na tržištu koji su u najboljem položaju da maksimalno smanje ili izbjegnu ostvarenje takvog rizika;
- **dobrovoljne ili obvezne sustave osiguranja:** takve bi se sustave moglo povezati s prethodno navedenim pristupima na temelju odgovornosti. U okviru njih strankama koje su pretrpjele štetu (npr. potrošaču) isplaćivale bi se naknade. Tim bi se pristupom trebala osigurati pravna zaštita za ulaganja poduzeća i istovremeno oštećenim osobama omogućiti pravednu naknadu ili primjereno osiguranje u slučaju štete.

U svakom bi se pristupu u obzir uzeli postupci pojedinca koji se služi tehnologijom i preciznije utvrdilo koja bi trebala biti uloga korisnika te tehnologije.

Komisija će se s dionicima savjetovati o prikladnosti postojećih pravila EU-a o odgovornosti u kontekstu interneta stvari i autonomnih povezanih sustava te o mogućim pristupima za prevladavanje postojećih poteškoća u dodjeli odgovornosti. Istovremeno se provodi i javno savjetovanje o općoj evaluaciji primjene Direktive o odgovornosti za proizvode. Komisija će procijeniti rezultate i razmotriti opcije za buduće djelovanje.

<sup>29</sup> Stroga odgovornost proizvođača u slučaju neispravnih proizvoda navedena je u drugim zakonodavnim aktima o sigurnosti proizvoda, na primjer u Direktivi o radijskoj opremi (2014/53/EU), uredbama o medicinskim proizvodima, Direktivi o strojevima (2006/42/EZ) i Direktivi o općoj sigurnosti proizvoda (2001/95/EZ).

<sup>30</sup> Komisija bi mogla izdati smjernice za primjenu pravila EU-a o odgovornosti na internet stvari i robotiku.

## **5. PRENOSIVOST, INTEROPERABILNOST I STANDARDI**

Druga nova pitanja u području podatkovnoga gospodarstva jesu prenosivost neosobnih podataka, interoperabilnost usluga u svrhu razmjene podataka i prikladni tehnički standardi za provedbu smislene prenosivosti.

### **5.1. Prenosivost neosobnih podataka**

Prenosivost podataka znači da potrošači i poduzeća mogu jednostavno prenijeti svoje podatke iz jednog sustava u drugi. Ona se u podatkovnom gospodarstvu općenito povezuje s niskim troškovima prebacivanja, a time i s niskim preprekama pristupu tržištu. Općom uredbom građanima će se osigurati pravo da dobiju osobne podatke proslijeđene pružatelju usluga u strukturiranom, uobičajenom i strojno čitljivom formatu i pravo da ih prenesu drugom pružatelju<sup>31</sup>.

Međutim, u pogledu neosobnih podataka u ovom trenutku ne postoje obveze kojima se jamči barem minimalna razina prenosivosti podataka, čak ni za internetske usluge u širokoj uporabi kao što su pružatelji usluga smještaja u oblaku. Razlog je tome djelomično to što zahtjevi za provedbu prenosivosti podataka mogu biti tehnički zahtjevni i skupi jer različiti pružatelji istih usluga podatke mogu pohranjivati različito.

U pogledu smislene prenosivosti neosobnih podataka u obzir bi trebalo uzeti i šira razmatranja upravljanja podacima, uključujući transparentnost za korisnike, upravljani pristup i interoperabilnost, u cilju povezivanja različitih platformi na načine kojima se potiču inovacije.

### **5.2. Interoperabilnost**

Razmatranja prenosivosti podataka često su blisko povezana s pitanjima njihove interoperabilnosti, zahvaljujući kojoj je moguća nesmetana razmjena podataka između više digitalnih usluga, a olakšavaju je primjerene tehničke specifikacije. U Direktivi o informacijama javnog sektora i povezanim smjernicama (uključujući Europski okvir interoperabilnosti) naglašava se koliko je važno da obogaćeni standardizirani metapodaci budu usklađeni s uspostavljenim rječnicima radi lakšeg pretraživanja i interoperabilnosti. Trenutačno se na prostorne podatke javnog sektora<sup>32</sup> primjenjuje Direktiva o infrastrukturi za prostorne informacije u Europskoj zajednici (INSPIRE) i povezane uredbe i smjernice o interoperabilnosti za prostorne podatke i povezane usluge, uključujući podatke pridobivene senzorima.

U slučaju internetskih platformi takvom se interoperabilnošću podataka ne olakšava samo prebacivanje, već i istovremena uporaba nekoliko platformi (tzv. „multi-homing”) te široko rasprostranjena razmjena podataka među platformama, što bi potencijalno moglo potaknuti inovacije u digitalnom gospodarstvu.

---

<sup>31</sup> Članak 20.

<sup>32</sup> Strojno generirani podaci smatraju se „prostornim podacima” jer senzori zajedno sa svojim mjerenjima obično prenose i svoj izravni ili neizravni položaj (lokaciju).

### 5.3. Standardi

Učinkovite politike o prenosivosti moraju biti popraćene prikladnim tehničkim standardima kako bi se smisljena prenosivost provela na tehnološki neutralan način. Komisija se obvezala<sup>33</sup> podržati prikladne standarde za poboljšanje interoperabilnosti, prenosivosti i sigurnosti usluga u oblaku boljom integracijom rada zajednica otvorenog koda u postupak utvrđivanja standarda na europskoj razini. Primjeri su takvog pristupa specifikacija TOSCA za aplikacije u oblaku, čiji je cilj unaprijediti prenosivost aplikacija i usluga u oblaku i njihovo operativno upravljanje<sup>34</sup> te tehničke specifikacije i smjernice provedbenih propisa o INSPIRE-u<sup>35</sup>.

### 5.4. Mogući smjerovi djelovanja

Mogući smjerovi djelovanja za rješavanje prethodno navedenih pitanja uključuju:

- **razvoj preporučenih uvjeta ugovora za olakšavanje promjene pružatelja usluga:** budući da su prenosivost podataka i promjena pružatelja podatkovnih usluga međusobno ovisni, mogao bi se ispitati razvoj standardnih uvjeta ugovora kojima se od pružatelja usluga zahtijeva provedba prenosivosti podataka potrošača;
- **razvoj daljnjih prava na prenosivost podataka:** na temelju prava na prenosivost podataka predviđenog Općom uredbom i predloženih pravila o ugovoru za opskrbu digitalnim sadržajem mogla bi se uvesti dodatna prava na prenosivost neosobnih podataka, posebno u kontekstu poslovanja među poduzećima, uzimajući pritom u obzir ishod provjere prikladnosti ključnih akata potrošačkog i tržišnog prava marketinga EU-a koja je u tijeku<sup>36</sup>.
- **eksperimentiranje sa standardima u određenom sektoru:** da bi se razvio čvrst pristup u području pravila o prenosivosti, utvrđenih u obliku standarda, mogli bi se pokrenuti eksperimentalni pristupi u pojedinačnim područjima. Oni bi općenito uključivali suradnju više dionika, među ostalim normizacijskih tijela, industrije, tehničke zajednice i javnih tijela.

Komisija će se savjetovati s dionicima o tim pitanjima i na temelju toga utvrditi je li potrebno daljnje djelovanje, možda u obliku prethodno navedenih djelovanja, bilo pojedinačno bilo kombinirano.

<sup>33</sup> COM(2016) 176 final: Prioriteti normizacije IKT-a za jedinstveno digitalno tržište

<sup>34</sup> <https://www.oasis-open.org/committees/tosca>

<sup>35</sup> Zakonodavstvo o INSPIRE-u: <http://inspire.ec.europa.eu/inspire-legislation/26>

<sup>36</sup> [http://ec.europa.eu/consumers/consumer\\_rights/review/index\\_en.htm](http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm)

## 6. EKSPERIMENTIRANJE I ISPITIVANJE

Eksperimentiranje je važan dio ispitivanja novih pitanja u podatkovnom gospodarstvu. Proučit će se mogućnost da se za potporu tim vrstama pokusa i eksperimenata upotrijebe financijska sredstva programa Obzor 2020.

Prije donošenja zaključaka o prikladnosti mogućih rješenja u pogledu pristupa podacima i odgovornosti trebalo bi organizirati posebno testiranje tih pitanja u stvarnom okruženju, u partnerstvu s dionicima. Potrebno je europsko rješenje utemeljeno na suradnji i eksperimentiranju među državama članicama.

S obzirom na prekograničnu dimenziju tog sektora, za takvo bi se testiranje mogla uzeti u obzir kooperativna, povezana i automatizirana mobilnost<sup>37</sup>

U nekoliko država članica već su u tijeku projekti za razvoj kooperativnih sustava i viših razina automatizacije<sup>38</sup>. Tim se projektima omogućuje povezivanje vozila međusobno i s cestovnom infrastrukturom kao što su semafori i prometni znakovi. Štoviše, Komisija zajedno sa skupinom zainteresiranih država članica namjerava utvrditi ispitni pravni okviri za eksperimentiranje na temelju usklađenih pravila o pristupu podacima i odgovornosti. Kako bi se omogućio pristup dovoljno velikoj količini podataka, testiranja bi trebalo temeljiti na tehnologiji 5G koja bi trebala nesmetano funkcionirati uz postojeće tehnologije koje se već uvode i u skladu s načelom komplementarnosti<sup>39</sup>.

Zanimljivo eksperimentiranje odvijat će se i u geoprostornom sektoru s nastankom novih podatkovnih ekosustava koji će temeljiti na programu za promatranje Zemlje Copernicus, trećem najvećem proizvođaču podataka na svijetu. Komisija razrađuje inovativna rješenja kako bi potaknula razvoj aplikacija na temelju programa Copernicus i drugih prostornih podataka, kojima će se prije svega obuhvatiti pitanja pristupa podacima, interoperabilnosti i predvidljivosti.

## 7. ZAKLJUČAK

Za stvaranje podatkovnoga gospodarstva EU-u je potreban okvir politike kojim se omogućuje uporaba podataka u cijelom vrijednosnom lancu u znanstvene, društvene i industrijske svrhe. U tu svrhu Komisija pokreće sveobuhvatan dijalog s dionicima o pitanjima koja su obuhvaćena ovom Komunikacijom. Prvi korak u tom dijalogu bit će javno savjetovanje. Pitanja pristupa podacima i odgovornosti ispitat će se i u stvarnom okruženju u području kooperativne, povezane i automatizirane mobilnosti.

Kad je riječ o slobodnom protoku podataka, Komisija će nastaviti raditi na tom pitanju u skladu s prethodno opisanim pristupom u cilju potpune provedbe načela slobodnog protoka podataka unutar EU-a, među ostalim i prioritarnim mjerama izvršenja kada to bude potrebno. Komisija će nastaviti i praćenje i prikupljanje dokaza te prema potrebi može razmotriti pokretanje dodatnih inicijativa za slobodan protok podataka.

---

<sup>37</sup> Vidi COM (2016) 766 od 30.11.2016.

<sup>38</sup> Vidi COM (2016) 766: Europska strategija za kooperativne inteligentne prometne sustave.

<sup>39</sup> Vidi COM (2016) 588: 5G za Europu: Akcijski plan.

Na temelju rezultata dijaloga s dionicima odlučit će i je li potrebno daljnje djelovanje u pogledu novih pitanja i u skladu s tim predložiti rješenja. U tom bi kontekstu eksperimentiranje u stvarnim uvjetima moglo imati važnu ulogu.