Primjene odredbi GDPR-a u prijenosu osobnih podataka izvan EU

Kordiš, Damir

LIBERTAS MEĐUNARODNO SVEUČILIŠTE
ZAGREB

PREDDIPLOMSKI STRUČNI STUDIJ

Primjene odredbi GDPR-a u prijenosu osobnih podataka izvan EU

KANDIDAT: Damir Kordiš
KOLEGIJ: Informacijska sigurnost
MENTOR: doc.dr.sc. Anita Perešin

Zagreb, ožujak, 2019.

KAZALO

Zahvala

Zahvaljujem svojoj obitelji na strpljenju i razumijevanju kako bi se ovaj završni rad realizirao. Nadalje, zahvaljujem dr.sc. Danielu Bari na izuzetno korisnim smjernicama vezanim uz ovaj završni rad.

1. UVOD

Informacija je temelj današnjeg društva. Od donošenja Direktive o zaštiti pojedinaca u vezi s obradom osobnih podataka, kao i o slobodnom protoku takvih podataka (*Direktiva 95/46/EZ Europskog parlamenta i vijeća*, u daljem tekstu: „Direktiva 95/46/EZ“) davne 1995. godine, svijet se značajno promijenio. Globalizacija poslovanja, razvoj interneta i značajno povećanje opće procesne snage računala doveli su do toga da se danas, više nego ikada ranije, prikuplja široki spektar osobnih podataka – od imena i adresa do detaljnih životnih navika, socijalnih i političkih stavova te podataka o zdravstvenom stanju. Temeljem tako prikupljenih podataka (engl. „*big data*“) provode se vrlo opsežna profiliranja za potrebe planiranja poslovnih ciljeva, primjene načela nove ekonomije, ciljanog marketinga te individualiziranog pristupa svakom kupcu. Mnoge organizacije smatraju osobne podatke ključnom vrijednošću bez koje ne bi mogle poslovati u modernom gospodarstvu. Kapital uvelike koristi blagodati globalizacije i alociranja poslovanja u zemlje gdje su troškovi rada značajno niži, tako da se poslovi obrade prikupljenih podataka često prenose u države koje nisu članice Europskog gospodarskog pojasa i izvan su izravne primjene prava Europske unije.

S druge strane, osim u pojedinim reguliranim izuzecima, svaki pojedinac ima pravo poštivanja svog osobnog života, života svoje obitelji i svoje komunikacije s drugima - jednom riječju pravo na privatnost. To je jedno od temeljnih ljudskih prava ugrađeno kako u ustave mnogih država tako i u zajedničke ustavne strukture Europske unije.

Prepoznavanjem problematike sve češćeg narušavanja navedenih osobnih prava, kao i prepoznavanjem nedostataka načela na kojima se direktive EU implementiraju u lokalna zakonodavstva država članica, Europska komisija je pristupila 2012. godine izradi Opće uredbe o zaštiti osobnih podataka (*Opća uredba o zaštiti podataka*, u daljem tekstu: „GDPR uredba“) u cilju harmonizacije pravila zaštite osobnih podataka kao te stvaranja pravne sigurnosti i transparentnosti poslovanja s gospodarskim subjektima na cijelom području Europske unije.

Nakon četiri godine pregovora, donošenjem GDPR uredbe, Europska komisija nametnula je visoke i unificirane standarde u postupanju s osobnim podacima građana Europske unije, te pravila obrade i prijenosa takvih podataka u općem teritorijalnom smislu. Svaki poduzetnik koji na bilo koji način obrađuje osobne podatke i na kojega se primjenjuju odredbe GDPR uredbe, u slučajevima povrede osobnih podataka uslijed nepridržavanja njenih odrednica izložen je visokim kaznama i drugim obvezama koje GDPR uredba propisuje, a koje ozbiljno mogu narušiti

svakodnevno poslovanje. Iz navedenih razloga potrebno je pomno razmotriti usklađenost obrade osobnih podataka s odredbama GDPR uredbe, kao i izloženost riziku povrede istih te poduzeti sve dostupne mjere kojima bi se taj rizik umanjio ili kontrolirao.

Zbog kompleksnosti primjene GDPR uredbe u svakodnevnom poslovanju koje uvelike nadilazi nacionalne granice, kao i zbog nedostatka relevantne literature, neka područja primjene GDPR uredbe nedovoljno su jednoznačno dokumentirana te kao takva podložna različitim tumačenjima. Jedno od takvih područja je i prijenos osobnih podataka u države izvan Europske unije.

Ovim radom će se ukazati na specifičnosti pravnog okvira međunarodnog prijenosa osobnih podataka u države izvan Europske unije, kao i na procjenu poslovnog rizika u okviru primjene odredbi GDPR uredbe te će biti ponuđen osvrt na organizacijske i pravne zahtjeve koji bi svojom primjenom u svakodnevnom poslovanju poduzetnika pridonijeli lakšem razumijevanju mehanizama upravljanja osobnim podacima u skladu s odredbama GDPR uredbe.

U radu se kao izvori podataka koriste zakonski akti, objave, znanstveni članci, interna dokumentacija tvrtke, te različite javno dostupne informacije.

Tijekom nastanka rada korištene su slijedeće metode istraživanja: analiza i sinteza, dedukcija, indukcija, komparacija, generalizacija i deskripcija.

Nakon uvodnog dijela rada, u drugom poglavlju pod nazivom *GDPR uredba* obrađen je povijesni razvoj zaštite osobnih podataka i prikaz bitnih odredbi GDPR uredbe. Treće poglavlje (*Pravni okvir međunarodnog prijenosa osobnih podataka trećim zemljama ili međunarodnim organizacijama*) pobliže analizira odredbe i mehanizme GDPR uredbe u slučajevima prijenosa osobnih podataka izvan Europske unije. U četvrtom poglavlju (*Procjena učinka na zaštitu podataka prilikom međunarodnog prijenosa osobnih podataka*) razmatraju se organizacijska rješenja u postupanju osoba odgovornih za sigurnost podataka u okviru odredbi GDPR uredbe. Peto poglavlje (*Postupanja u slučajevima povrede osobnih podataka*) analizira postupanje poduzetnika u slučajevima povrede osobnih podataka. Na kraju rada izveden je sveobuhvatan zaključak.

2. GDPR UREDBA

2.1. Povijesni razvoj zaštite osobnih podataka i razlozi donošenja GDPR uredbe

Pravo na zaštitu osobnih podataka jedno je od temeljnih prava svakog čovjeka. Svrha zaštite osobnih podataka je zaštita privatnog života te ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka.

Ne ulazeći u dalju povijest, razvoj prava na zaštitu osobnih podataka započinje definiranjem zaštite prava na privatnost u članku 12. Opće deklaracije Ujedinjenih naroda o ljudskim pravima, gdje se navodi: „Nitko ne smije biti podvrgnut samovoljnom miješanju u njegov privatni život, obitelj, dom ili dopisivanje, niti napadima na njegovu čast i ugled. Svatko ima pravo na zakonsku zaštitu protiv takvog miješanja ili napada.“ (*Opća deklaracija o ljudskim pravima*, Rezolucija Ujedinjenih naroda br. 217 /III)

Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda (*Konvencija za zaštitu ljudskih prava i temeljnih sloboda-pročišćeni tekst*), u članku. 8. navodi kako svatko ima pravo na poštivanje svog osobnog i obiteljskog života, prebivališta i dopisivanja.

Vijeće Europe Konvencijom za zaštitu osoba glede automatizirane obrade osobnih podataka (*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, dalje u tekstu: „ETS br. 108.“), utvrđuje pravni okvir kojim sve države potpisnice svakoj fizičkoj osobi osiguravaju poštovanje njezinih prava i temeljnih sloboda, osobito njezino pravo na privatnost glede automatizirane obrade osobnih podataka koji se na nju odnose, a Dodatnim protokolom uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u svezi nadzornih tijela i međunarodne razmjene podataka (*Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*, dalje u tekstu: „ETS br. 181.“) dodatno se učvršćuje zaštitu osobnih podataka kroz obavezu državama potpisnicama za osnivanje nacionalnih nadzornih tijela i stvara pravni okvir prijenosa osobnih podataka u treće zemlje.

U Povelji Europske unije o temeljnim pravima (*2012/C 326/02*), zasebno se u članku 7. i članku 8. izdvaja pravo na zaštitu osobnih podataka od prava na privatnost.

Svojevrstan temelj GDPR uredbe nalazimo u ranijoj Direktivi 95/46/EZ Europskog parlamenta i Vijeća o zaštiti pojedinaca u području obrade osobnih podataka te o slobodnom protoku takvih podataka. Načelo na kojem se odredbe direktive Europske unije primjenjuju u lokalnim zakonodavstvima država članica dovelo je do različitog tumačenja odredbi Direktive 95/46/EZ stvarajući niz sličnih, ali ne jedinstvenih uvjeta poštivanja zaštite osobnih podataka. Uslijed toga, poslovni subjekti i organizacije koje posluju na području Europskog gospodarskog pojasa na načelu slobodnog prometa roba i usluga, suočavaju se s različitim zahtjevima za usklađivanjem između država članica.

Europska Komisija 2016. godine donosi GDPR uredbu *(*engl. „*General Data Protection Regulation*“ ili „*GDPR*“), punim nazivom Opća uredba o zaštiti pojedinca u vezi s obradom osobnih podataka i slobodnom kretanju takvih podataka, kojom ujedno stavlja izvan snage Direktivu 95/46/EZ, kako bi ujednačila i zaštitila slobode na koje njeni građani imaju pravo na cijelom području Europske unije. GDPR uredba, koja je ušla u punu primjenu 25. svibnja 2018. godine, regulira obradu osobnih podataka građana Europske unije sa strane pojedinca, trgovačkog društva ili organizacije u Europskoj uniji.

Republika Hrvatska, kao članica Vijeća Europe, potpisnica je Konvencije ETS br. 108. i dodatnog protokola ETS br. 181., koje ratificira Zakonom o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i dodatnog protokola uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka (*NN, br. 4/05*). Područje zaštite osobnih podataka u okviru navedenih normi EU zakonski je regulirano u RH Zakonom o zaštiti osobnih podataka (*NN, br. 103/03*) i naknadno unaprijeđeno njegovim dopunama (*NN, br. 118/06, 41/08 i 130/11*).

Hrvatski sabor je na svojoj sjednici 27. travnja 2018. godine donio Zakon o provedbi Opće uredbe o zaštiti podataka (*NN, br 42/18*), kojim se osigurava provedba GDPR uredbe i imenuju nacionalna provedbena tijela.

2.2. GDPR uredba

GDPR uredba sastoji se od 173 uvodne izjave u preambuli i 99 operativnih odredbi podijeljenih u jedanaest poglavlja. Dok uvodne izjave nemaju pravni efekt i služe kao pojašnjenja operativnim odredbama GDPR uredbe, operativne odredbe imaju punu pravnu primjenu u svim državama članicama. GDPR uredba kao takva ne zahtijeva implementaciju u

lokalna zakonodavstva iako omogućava državama članicama određena prava derogiranja njenih odredbi. Ovo pravo državama članicama omogućava samostalno reguliranje pitanja vezanih uz nacionalnu sigurnost, prevenciju i otkrivanje kriminalnih aktivnosti te ostale javne interese.

GDPR uredbom se štite temeljna prava i slobode pojedinca u odnosu na zaštitu njegovih osobnih podataka uz kontrolu prijenosa istih unutar i izvan Europske unije. Uredba se primjenjuje na obradu osobnih podataka kada je predmetna obrada potpunosti ili djelomično automatizirana, kao i na neautomatiziranu obradu koja čini dio sustava pohrane ili je namijenjena biti dio istog sustava. Ona se odnosi na obradu osobnih podataka u okviru aktivnosti izvršitelja s poslovnim nastanom u Europskoj uniji, ali i na izvršitelja izvan Europske unije ukoliko je obrada povezana s nuđenjem roba i usluga te praćenjem ponašanja ispitanika dok se njihove aktivnosti odvijaju unutar Europske unije. Međutim, kao posljedica globalizacije svakodnevno raste količina osobnih podataka koje tijela država članica, organizacije, poduzeća i privatne osobe prenose u zemlje izvan Europske unije, tako da se GDPR uredbom uspostavljaju mehanizmi zaštite tako prenesenih podataka ukoliko se obrada vrši izvan država članica.

GDPR uredba jednoznačno daje definicije pojmova koji su bitni za razumijevanje daljih aspekata njene primjene na zaštitu osobnih podataka.

Pojmom *osobni podaci* obuhvaćeni su svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik“) to jest na osobu koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator te uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca. Sveobuhvatni pregled osobnih podataka, grupiranih prema najčešće primjenjivanoj kategorizaciji, prikazan je u Prilogu 1.

Obrada je svaki postupak ili skup postupaka koji se obavljaju s osobnim podacima ili sa skupovima osobnih podataka, bilo automatiziranim ili neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje.

Sustav pohrane je svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi.

Voditelj obrade je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom EU ili pravom države članice. Voditelj obrade te posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom EU ili pravom države članice.

Izvršitelj obrade je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade.

Primatelj je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podatci, neovisno o tome je li on treća strana.

Treća strana je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade niti osoba ovlaštena za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade.

Privola ispitanika je svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika, gdje on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.

Povreda osobnih podataka je kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podatcima koji su preneseni, pohranjeni ili na drugi način obrađivani.

Glavni poslovni nastan je:

(a) što se tiče voditelja obrade s poslovnim nastanima u više od jedne države članice, glavni poslovni nastan je mjesto njegove središnje uprave u Uniji, osim ako se odluke o svrhama i sredstvima obrade osobnih podataka donose u drugom poslovnom nastanu voditelja obrade u Europskoj uniji te je potonji poslovni nastan ovlašten provoditi takve odluke, u kojem se slučaju poslovni nastan u okviru kojeg se donose takve odluke treba smatrati glavnim poslovnim nastanom.

(b) što se tiče izvršitelja obrade s poslovnim nastanima u više od jedne države članice, glavni poslovni nastan je mjesto njegove središnje uprave u Uniji, ili, ako izvršitelj obrade nema središnju upravu u Uniji, poslovni nastan izvršitelja obrade u Uniji u kojem se odvijaju glavne aktivnosti obrade u kontekstu aktivnosti poslovnog nastana izvršitelja obrade u mjeri u kojoj izvršitelj obrade podliježe posebnim obvezama u skladu s ovom GDPR uredbom.

Predstavnik je fizička ili pravna osoba s poslovnim nastanom u EU koju je voditelj ili izvršitelj obrade imenovao pisanim putem u skladu s člankom 27. GDPR uredbe, a koja predstavlja voditelja ili izvršitelja obrade u pogledu njihovih obveza na temelju GDPR uredbe.

Poduzeće je fizička ili pravna osoba koja se bavi gospodarskom djelatnošću, bez obzira na pravni oblik te djelatnosti, uključujući partnerstva ili udruženja koja se redovno bave gospodarskom djelatnošću.

Poštujući načela GDPR uredbe, obrada osobnih podataka (poglavlje II, članak 5. do 11.) mora biti zakonita, poštena i transparentna („**zakonitost, poštenost i transparentnost**“) u odnosu na ispitanika te se ovako prikupljani podatci moraju koristiti u posebne, izričite i zakonite svrhe **(„ograničavanje svrhe“)** i ne smiju se dalje obrađivati na način koji nije u skladu sa tim svrhama. Nadalje, opseg prikupljenih podataka mora biti primjeren, relevantan i ograničen („**smanjenje količine podataka**“) na samu svrhu prikupljanja i obrade. Osobni podaci moraju biti točni i po mogućnosti ažurni („**točnost**“), te se moraju poduzeti sve razumne mjere kako bi se podaci koji nisu točni ili ažurni u odnosu na svrhu obrade, izbrisali ili ispravili. Osobni podaci kroz koje je moguća identifikacija ispitanika moraju biti čuvani samo onoliko dugo koliko je potrebno u svrhe obrade za koje su podaci prikupljani („**ograničenje pohrane**“), osiguravajući za cijelo vrijeme obrade odgovarajuću sigurnost, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja („**cjelovitost i povjerljivost**“).

Zakonitost obrade utvrđuje se ukoliko je voditelj obrade u mogućnosti dokazati kako je ispitanik dao privolu za obradu svojih osobnih podataka. Obrada osobnih podataka je nužna radi pravnih obaveza voditelja obrade kako bi se zaštitili ključni interesi ispitanika i/ili drugih osoba, kao i za izvršavanje zadaća od javnog interesa. GDPR uredbom se načelno zabranjuje obrada posebnih kategorija osobnih podataka[1]. Međutim obrada posebnih kategorija osobnih podataka dopustiva je u određenim okolnostima uz primjenu odgovarajućih zaštitnih mjera - u radnom pravu, socijalnom pravu te u svrhu javne zdravstvene zaštite.

GDPR uredba nadalje osigurava veća prava ispitanika te mu omogućava višu razinu kontrole nad obradom svojih osobnih podataka koju provode voditelj ili izvršitelj obrade. U smislu GDPR uredbe ovaj skup prava objedinjuje se pod pojmom „Prava ispitanika“. **Pravo na informiranost** podupire osnovni koncept transparentnosti, komunikacije i modaliteta za ostvarivanje prava ispitanika, te je sastavni dio poštivanja načela zakonitosti, poštenosti i transparentnosti obrade osobnih podataka. **Pravo pristupa** je jedno od najznačajnijih prava

[1] Pogledati prilog 1: Kategorizacija osobnih podataka, str. 29.

ispitanika koje donosi GDPR uredba. Ono donosi ispitaniku pravo potvrde da se njegovi osobni podaci obrađuju na zakonit način u razumnom roku. Ovo pravo je usko povezano s ispitanikovim pravom na **prenosivost podataka** čime ispitanik može zahtijevati i zaprimati podatke koji se odnose na njega, a koje je dao voditelju obrade u strukturiranom, standardno upotrebljavanom i strojno čitljivom obliku, te tako primljene podatke može prenijeti drugom voditelju. **Pravo na ispravak** daje ispitaniku mogućnost ispravka ili dopune osobnih podataka koje voditelj obrađuje, a tako zatražene izmjene i/ili dopune voditelj treba evidentirati bez odgode. **Pravo na brisanje** ili **pravo na zaborav** omogućava ispitaniku zahtijevati od bilo kojeg voditelja obrade brisanje njegovih osobnih podataka u određenim okolnostima kao što su povlačenje suglasnosti ispitanika za obradu njegovih osobnih podataka ukoliko osobni podatci više nisu potrebni za svrhu za koju su inicijalno prikupljeni ili ukoliko su osobni podatci nezakonito obrađivani. Kada je voditelj obrade objavio osobne podatke koje je obavezan obrisati, on mora poduzeti razumne korake kako bi obavijestio ostale voditelje obrade o zahtjevu ispitanika za brisanjem. Brisanje u tom slučaju uključuje i poveznice na osobne podatke koji se brišu kao i sve kopije ili replike istih. Ova funkcija po mnogima daje pojmu „pravo na zaborav“ pravi smisao. **Pravo na ograničenje obrade** pruža ispitaniku pravo zahtijevati od voditelja obrade ograničavanje njegovih osobnih podataka. Brisanje može biti privremeno, u slučajevima kada ispitanik dovodi u pitanje ispravnost osobnih podataka ili se pozvao na pravo prigovora, odnosno trajno kada se radi o nezakonitoj obradi, a ispitanik se ne protivi brisanju ili u slučaju da voditelj obrade više ne treba osobne podatke u svrhu obrade ali ih ispitanik traži radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva. Ispitanik ima **pravo na prigovor** u tri slučaja, a voditelj obrade tada mora zaustaviti daljnju obradu. Radi se o u slučaju kada se osobni podaci obrađuju u svrhu izravnog marketinga, uključujući profiliranje. U drugom slučaju osobni se podaci obrađuju u sklopu znanstvenih i povijesnih istraživanja te u statističke svrhe, a treći slučaj nastupa kada je dovedena u pitanje zakonitost obrade u svrhu zadaća od javnog interesa, ili su dovedene u pitanje službene ovlasti i legitimni interesi voditelja obrade ili treće strane. **Prava koja se odnose na automatizirano odlučivanje i profiliranje** ispitaniku daju mogućnost zahtjeva da se na njega ne odnose odluke s pravnim učinkom na njega, a koje se temelje na isključivo automatiziranoj obradi, uključujući izradu profila.

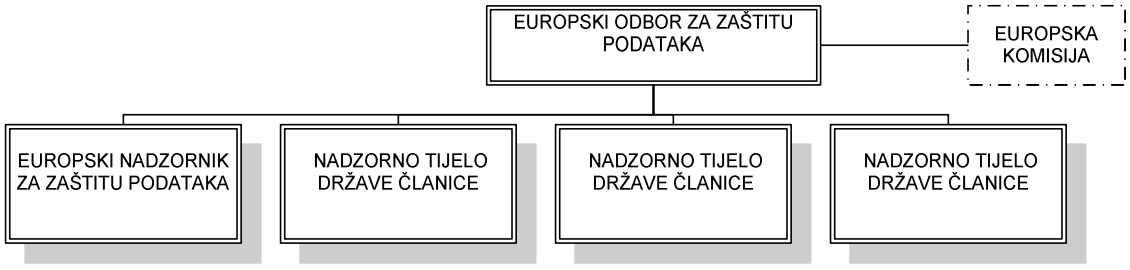
2.3. Tijela provedbe GDPR uredbe

GDPR uredba postavlja zahtjev ispred svake države članice za imenovanjem neovisnog nadzornog tijela odgovornog za praćenje usklađenosti sa GDPR uredbom na nacionalnoj razini.

U Republici Hrvatskoj Zakon o provedbi Opće uredbe o zaštiti podataka (*NN, br. 42/18*) jedinim neovisnim tijelom imenuje Agenciju za zaštitu osobnih podataka (dalje u tekstu: „AZOP“) sa sjedištem u Zagrebu. AZOP djeluje potpuno neovisno pri obavljanju svojih zadaća i izvršavanju ovlasti sukladno odredbama GDPR uredbe.

Kako bi se osigurala konzistentna primjena odredbi GDPR uredbe na cijelom području Europske unije, kao centralno tijelo Europske unije osniovan je Europski odbor za zaštitu podataka u svojstvu pravne osobe koja djeluje neovisno u praćenju i osiguravanju pravilne primjene odredbi GDPR uredbe te očuvanju mehanizma konzistentnosti u slučajevima sporova između različitih razina nadzornih tijela. Odbor također daje mišljenja o mjerama nadzornih tijela država članica koje mogu imati utjecaj na jedinstvenost primjene odredbi GDPR uredbe u državi članici. Europski odbor za zaštitu podataka čine po jedan predstavnik nadzornog tijela iz svake države članice, zatim predstavnik Europskog nadzornika za zaštitu podataka i predstavnik Europske komisije. Predstavnici nadzornih tijela država članica i predstavnik Europskog nadzornika za zaštitu podataka (tijelo zaduženo za osiguravanje poštivanja prava građana na privatnost pri obradi njihovih osobnih podataka od strane institucija i tijela EU-a) aktivno sudjeluju u postizanju jedinstvenosti stavova u odnosu na odredbe GDPR uredbe na cijelom području Europske unije, dok predstavnik Europske komisije u radu Europskog odbora za zaštitu podataka sudjeluje kao pridruženi član bez prava glasa, te je njegova isključiva uloga koordinacija s Europskom komisijom. U prikazu 1. vidljiva je organizacijska struktura Europskog odbora za zaštitu podataka.

Prikaz 1: Organizacijska struktura Europskog odbora za zaštitu podataka



Izvor: Sistematizacija autora (2018)

U skladu s odredbama GDPR uredbe, u cilju konzistentnosti nadzora provedbe odredbi GDPR uredbe, nadzor aktivnosti prekogranične obrade ili obrade koja uključuje građane više od jedne države Europske unije u pravilu vodi samo jedno nadzorno tijelo koje se naziva vodeće nadzorno tijelo. Vodeće nadzorno tijelo prvenstveno je odgovorno za nadzor aktivnosti prekogranične obrade, poput slučajeva kad se istražuje društvo koje obavlja aktivnost obrade u nekoliko država članica. Vodeće nadzorno tijelo koordinira postupke u koje su uključena druga nadzorna tijela u skladu s načelima jedinstvenog mehanizma, uzajamne pomoći predmetnih nadzornih tijela i prema potrebi vodi zajedničke operacije. Nacrti svih odluka dostavljaju se nadzornim tijelima zainteresiranima za predmet, koja donose konzistentne odluke o predmetu. U prikazu 2. vidljiva je organizacijska struktura suradnje vodećeg nadzornog tijela i predmetnih nadzornih tijela u državama članicama.

Prikaz 2: Suradnja vodećeg nadzornog tijela i drugih predmetnih nadzornih tijela

Izvor: Sistematizacija autora (2018)

2.4. Pravna sredstva, odgovornost i sankcije

Sukladno Članku 47. Povelje Europske Unije o temeljnim pravima: „svatko čija su prava i slobode zajamčeni pravnom stečevinom Unije prekršeni, ima pravo na pravično, javno suđenje u razumnom vremenskom roku pred neovisnim i nepristranim sudom, prethodno osnovanim u skladu sa zakonom“ *(2016/C 202/02*). Svatko ima mogućnost da bude savjetovan, branjen i zastupan te se onima koji nemaju dostatna sredstva osigurava pravna zaštita kako bi svi imali učinkovit pristup pravosuđu.

GDPR uredba svojim odredbama ispitaniku daje pravo pritužbe nadzornom tijelu ukoliko smatra da su mu narušena prava iz GDPR uredbe. Pritužbe na pravno obvezujuće odluke

nadzornog tijela vode se ispred sudova države članice u kojoj nadzorno tijelo ima poslovni nastan.

Odredbama GDPR uredbe definira se, uz izricanje upravnih novčanih kazni, i odgovornost voditelja i/ili izvršitelja obrade, a svaka osoba koja je zbog kršenja odredbi GDPR uredbe pretrpjela materijalnu ili nematerijalnu štetu ima pravo na naknadu tako nastale štete. Za tako nastalu štetu solidarno odgovaraju voditelj obrade, izvršitelj obrade, više voditelja i izvršitelja obrade, te ukoliko jedan od njih nadoknadi cjelokupnu štetu oštećenoj osobi, isti zadržava pravo regresa[2] od drugih sudionika koji su učestvovali u obradi.

Općim uvjetima za izricanje upravnih novčanih kazni u GDPR uredbi se određuju jedinstvene upravne kazne na razini cijele Europske unije, što se smatra glavnim pokretačem stvarnog i dosljednog pridržavanja odredbi GDPR uredbe te ih je bitno posebno istaknuti.

a) „Za kršenje slijedećih odredbi… mogu se izreći upravne novčane kazne u iznosu do 10.000.000 EUR, ili u slučaju poduzetnika do 2% ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće:… **kod kršenja obaveza voditelja obrade i izvršitelja obrade** u odnosu na uvjete koji se primjenjuju na privolu djeteta u svezi usluga informacijskog društva, obrada koje zahtijevaju identifikaciju, neprovođenja adekvatnih mjera tehničke i integrirane zaštite podataka, neuspostavljanja dogovora oko odgovornosti u slučajevima zajedničkih voditelja obrade, propuštanje imenovanja predstavnika voditelja ili izvršitelja obrade u Europskoj uniji za voditelja ili izvršitelja obrade čiji je poslovni nastan izvan Europske unije, kršenja obveza izvršitelja obrade u provedbi obrade za voditelja obrade, šire obrade osobnih podataka izvršitelja obrade nego što je to od izvršitelja zatražio voditelj obrade, **kod kršenja obaveza certifikacijskog tijela** kod izdavanja praćenja i reizdavanja certifikata o sigurnosti obrade osobnih podataka voditeljima i/ili izvršiteljima obrade, **kod kršenja obaveza tijela** za praćenje uspostavljenog kodeksa ponašanja voditelja i/ili izvršitelja obrade.“ (2*016/679, članak 83. stavak 4*).
b) „Za kršenje slijedećih odredbi… mogu se izreći upravne novčane kazne u iznosu do 20.000.000 EUR, ili u slučaju poduzetnika do 4% ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće:…**kod kršenja osnovnih načela privole** u odnosu na načela obrade osobnih podataka,

[2] Regresno pravo je pravo osobe koja je podmirila neki iznos umjesto druge osobe, da taj iznos, ili dio iznosa, potražuje od te druge osobe (tumačenje autora).

zakonitosti obrade, uvjeta privole i obrade posebnih kategorija osobnih podataka, **kod kršenja prava ispitanika** u odnosu na transparentnost i modalitete obrade, informiranost i pristup osobnim podacima, ispravak i brisanje te pravo na prigovor i automatizirano pojedinačno donošenje odluka, kršenja odredbi GDPR uredbe pri **prijenosu osobnih podataka** primatelju u trećim zemljama ili međunarodnim organizacijama, **kod kršenja svih obaveza u skladu s pravom države članice** donesenim na temelju poglavlja IX (posebne situacije obrade), **kod nepoštovanja naredbe** nadležnog tijela za suspenziju protoka podataka ili privremenu odnosno trajnu obustavu postupaka obrade, naputaka nadležnog tijela za korekcijama i onemogućavanja ovlasti nadležnog tijela“ (*2016/679, članak 83. stavak 5*).

Kod izricanja gore navedenih upravnih kazni nadzorno tijelo osigurava da su iste u svakom pojedinačnom slučaju učinkovite, proporcionalne i odvraćajuće, uzimajući posebno u obzir, između ostalih okolnosti kršenja, prirodu, težinu i trajanje kršenja u kontekstu naravi, opsega i svrhe obrade, kategorije osobnih podataka na koje se kršenje odnosi, jesu li su kršenja namjerna ili nenamjerna i koje postupke je voditelj ili izvršitelj poduzeo kako bi ublažio nastalu štetu.

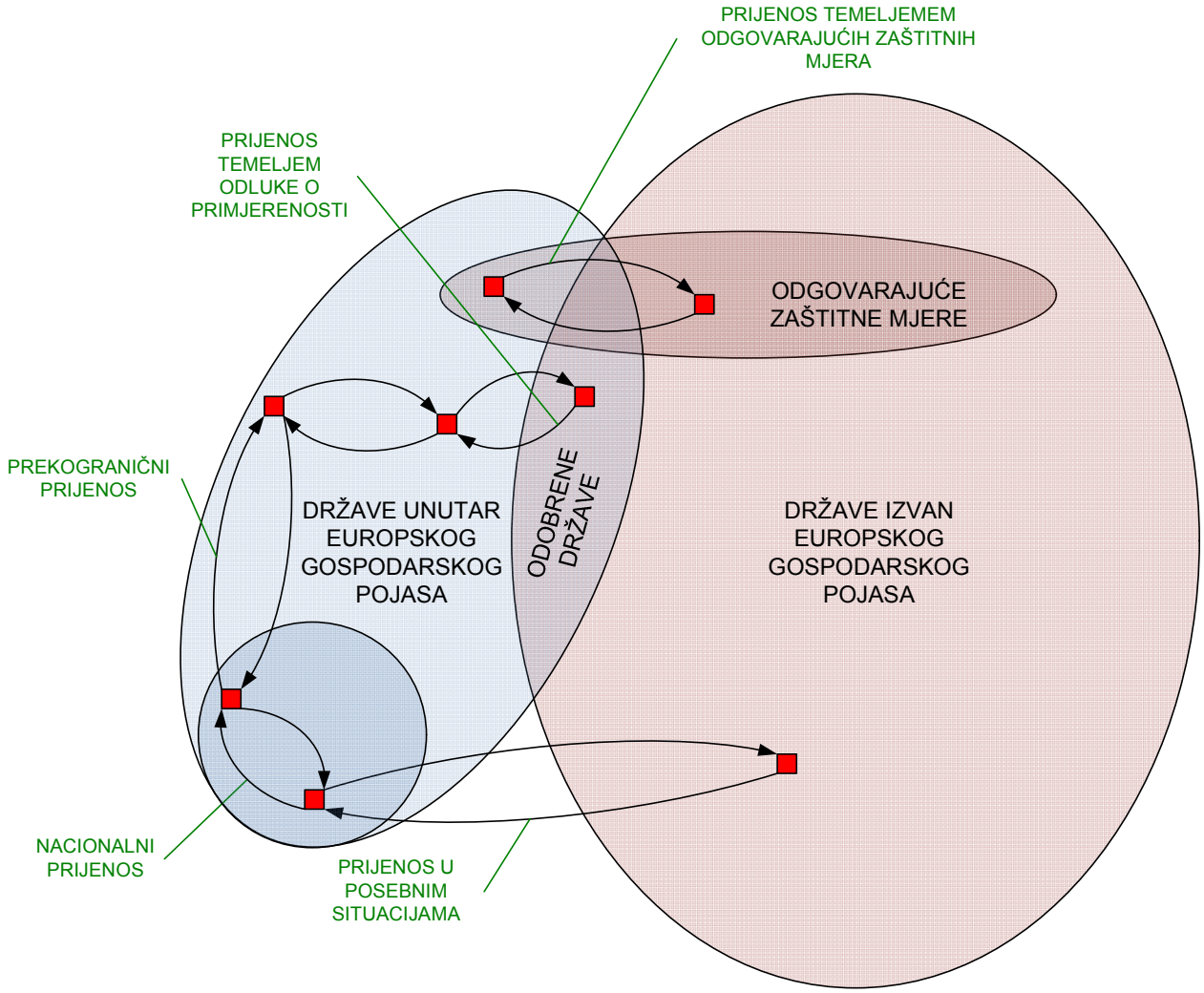
Prikaz 3: Grafički prikaz osnovnih elemenata GDPR uredbe

Izvor: https://teachprivacy.com/gdpr-whiteboard/

3. PRAVNI OKVIR MEĐUNARODNOG PRIJENOSA OSOBNIH PODATAKA TREĆIM ZEMLJAMA ILI MEĐUNARODNIM ORGANIZACIJAMA

Europska komisija (dalje u tekstu: „EK“) u Komunikaciji Europskom parlamentu i vijeću (*Razmjena i zaštita osobnih podataka u globaliziranom svijetu*, 2017.) utvrđuje se strateški okvir Europske komisije za odluke o primjerenosti i druge primjenjive alate za prijenos osobnih podataka te međunarodne instrumente za njihovu zaštitu, dok se samim odredbama GDPR uredbe (članak 45., stavak 1.) postavlja osnovni princip kojim se prijenos osobnih podataka u treće države ili međunarodne organizacije može provoditi ukoliko treća država, teritorij ili sektor gdje se osobni podaci prenose može osigurati adekvatnu razinu zaštite.

Prikaz 4: Načini prijenosa osobnih podataka



Izvor: Sistematizacija autora (2018)

Kako je prikazano u Prikazu 4., prijenosi osobnih podataka između voditelja ili voditelja i izvršitelja obrade u okviru GDPR uredbe mogu se odvijati na nacionalnoj razini unutar države članice, unutar Europskog gospodarskog pojasa, te izvan njega. Kod prijenosa osobnih podataka na nacionalnoj razini ili unutar Europskog gospodarskog pojasa osigurana je puna primjena odredbi GDPR uredbe, dok kod prijenosa osobnih podataka u treće države GDPR uredba predviđa specifične okolnosti i uvjete pod kojima se takav prijenos može izvršavati. Prijenos osobnih podataka u treće države dozvoljen je temeljem odluke o primjerenosti, gdje je EK donijela odluku da se u predmetnim trećim državama ispitaniku može garantirati primjerena zaštita osobnih podataka, primjenom odgovarajućih zaštitnih mjera kojima voditelj ili izvršitelj obrade s poslovnim nastanom unutar Europskog gospodarskog pojasa uspostavlja pravni okvir s izvršiteljem obrade izvan Europskog gospodarskog pojasa. U posebnim situacijama, prijenos

osobnih podataka dozvoljava se izvan Europskog gospodarskog pojasa ukoliko je svrha prijenosa neka od okolnosti koje GDPR uredba eksplicitno navodi.

3.1. Prijenosi temeljem odluke o primjerenosti

Jedan od mehanizama prijenosa osobnih podataka izvan Europskog gospodarskog pojasa je prijenos na temelju „Odluke o primjerenosti“ EK kojom se potvrđuje da država izvan Europskog gospodarskog pojasa pruža razinu zaštite osobnih podataka koja je „bitno ekvivalentna“ zaštiti u Europskoj uniji (*C362/14*). Prijenos podataka temeljem Odluke o primjerenosti omogućen je bez potrebe za daljim zaštitnim mjerama ili ishođenjem dozvola.

Odluka o primjerenosti donosi se na osnovi procjene EK koja mora uzimati u obzir vladavinu prava, poštivanje ljudskih prava i temeljnih sloboda te relevantno zakonodavstvo, posebice zakonodavstvo u području zaštite osobnih podataka, javne sigurnosti, obrane, nacionalne sigurnosti i kaznenog prava, kao i pristup tijela javne vlasti osobnim podacima. Nadalje, u razmatranje ulaze i provedivost i djelotvornost sudske i upravne vlasti u provođenju zakona koji se odnose na zaštitu osobnih podataka, kao i pripadnost i provođenje pravno obvezujućih Konvencija EU, posebice Konvencije br. 108. i njenih dopuna (*ETS br. 108*.“ i *ETS br. 181*) Vijeća Europe i drugim regionalnim sustavima koji se bave zaštitom podataka.

Odlukom o primjerenosti EK utvrđuje da dotična država pruža razinu zaštite osobnih podataka koja je usporediva razini zaštite koju pruža EU. Posljedično se prijenos osobnih podataka u te države izjednačava s prekograničnim prijenosom podataka unutar Europske unije. Kao primjerene razine zaštite EK može priznati razne sustave zaštite privatnosti uvažavajući različitosti u pravnim okruženjima, ukoliko navedeni sustavi pružaju adekvatan standard zaštite koji nije nužno istovjetan pravilima unutar Europske unije. Odluke o primjerenosti odnose se na države koje su usko povezane s EU i njenim članicama (Švicarska, Andora, Farski Otoci, Guernsey, Jersey, Otok Man), koji su važni trgovinski partneri Europske unije (Argentina, Kanada, SAD, Izrael) ili su države koje imaju istaknutu ulogu u širenju i učvršćivanju zakona o zaštiti podataka u svojim regijama (Novi Zeland, Urugvaj). Donošenje Odluke o primjerenosti uključuje poseban dijalog i blisku suradnju s predmetnom trećom državom.

U svojim razmatranjima EK može donositi odluku o primjerenosti na razini cijele države, zatim na razini djelomične primjerenosti ili sektorske primjerenosti (npr. za sektor financija, IT).

Samo usvajanje odluke o primjerenosti uključuje:

- prijedlog Europske komisije;
- mišljenje Europskog odbora za zaštitu podataka;
- odobrenje predstavnika država članica;
- donošenje odluke europskih povjerenika.

Čak i nakon donošenja odluke o primjerenosti, EK je obavezna pratiti i nadzirati događaje koji mogu utjecati na razinu zaštite osobnih podataka koje osigurava predmetna država. U tu svrhu provodi se periodično preispitivanje Odluke o primjerenosti, a EK je obavezna provesti preispitivanje svake pojedine odluke o primjerenosti najmanje jednom u četiri godine.

U određenim situacijama EK može donijeti o određene specifične i nepotpune odluke o primjerenosti. Neke od njih su bitne trgovinske partnere Europske unije, kao npr. odluke o primjerenosti u odnosu na Kanadu i SAD, koje nisu potpune. To znači kako je prije prijenosa osobnih podataka u navedene države potrebno obratiti posebnu pozornost na dio Odluke na koji se ona odnosi. Na primjer, Odluka o primjerenosti za Kanadu odnosi se samo na privatne subjekte (ispitanike) koji su obuhvaćeni područjem primjene kanadskog *Zakona o zaštiti osobnih podataka i elektroničkim dokumentima,* dok je Odluka o primjerenosti europsko-američkog sustava zaštite privatnosti i osobnih podataka specifična zbog različitosti zakonodavstva u području zaštite osobnih podataka unutar SAD, odnosno zbog nedostatka općeg i jedinstvenog federalnog zakona. Odluka o primjerenosti u odnosu na SAD temelji se na obavezama poduzeća koja sudjeluju u sustavu samocertificiranja i primjene visokih standarda zaštite osobnih podataka.

Odluka o primjerenosti jednostrana je provedbena odluka EK koja se donosi u skladu s pravom Europske unije o zaštiti podataka te ni u kojem slučaju ne može biti predmet bilo kojih drugih trgovinskih sporazuma.

3.2. Prijenosi koji podliježu odgovarajućim zaštitnim mjerama

U nedostatku odluke o primjerenosti, osobni podaci mogu se prenijeti izvan Europskog gospodarskog pojasa ako je voditelj obrade ili izvršitelj obrade: "... predvidio odgovarajuće

zaštitne mjere i pod uvjetom da su ispitanicima na raspolaganju provediva prava i učinkovita sudska zaštita" (*GDPR uredba, Članak 46*.).

Direktiva navodi slijedeće "odgovarajuće zaštitne mjere":

- pravno obvezujući i provedivi instrument između javnih tijela
- obvezujuća korporativna pravila
- standardne ugovorne odredbe koje je usvojila EK
- standardne ugovorne odredbe koje donosi nadzorno tijelo i koje odobrava EK
- odobreni kodeks ponašanja
- odobreni mehanizam certificiranja

Od gore navedenih zaštitnih mjera najčešće se koriste standardne ugovorne klauzule (engl. „*model contract clauses*“) koje je usvojila EK za voditelje obrade koji osobne podatke prenose voditelju ili izvršitelju obrade u trećim zemljama i obvezujućih korporativnih pravila gdje se osobni podaci prenose unutar grupe poduzetnika ili interesne grupe poduzeća.

3.3. Standardne ugovorne klauzule

Temeljem provedenog postupka ispitivanja, EK donosi standardne ugovorne klauzule koje propisuju da država članica može odobriti prijenos osobnih podataka u treću državu koja ne osigurava odgovarajuću razinu zaštite, odnosno kada treća država nije obuhvaćena odlukom o primjerenosti.

Standardne ugovorne klauzule predstavljaju ugovorni mehanizam u smislu zaštitne mjere kod međunarodnog prijenosa osobnih podataka. Do sada je EK izdala dva paketa standardnih ugovornih klauzula za prijenos osobnih podataka od voditelja obrade u Europskoj uniji drugom voditelju obrade u trećoj zemlji (*Odluka Komisije od 15. lipnja 2001.* i *Odluka Komisije od 27. prosinca 2004*.) i jedan paket za prijenos osobnih podataka od voditelja obrade u Europskoj uniji izvršitelju obrade u trećoj zemlji (*Odluka Komisije od 5. veljače 2010*.). Ove standardne

ugovorne klauzule donesene su sukladno članku 26., stavak 4. Direktive 95/46/EZ, te iste ostaju na snazi dok EK iste po potrebi izmijeni, zamijeni ili stavi izvan snage.

Standardne ugovorne klauzule može donijeti i nadzorno tijelo države članice, ali uz prethodnu konzultaciju s EK.

3.4. Obvezujuća korporativna pravila

GDPR uredba daje mogućnost grupi poduzetnika ili tvrtki koje se bave zajedničkom gospodarskom aktivnošću donošenja obvezujućih korporativnih pravila (engl. „*binding corporate rules*“ ili „*BCR*“) kojima se uređuju pitanja zaštite osobnih podataka prilikom prijenosa osobnih podataka unutar grupe poduzetnika. Obvezujuća korporativna pravila predstavljaju neku vrstu internog pravilnika postupanja s osobnim podacima, najčešće prilikom prijenosa osobnih podataka u okviru multinacionalnih kompanija.

Pritom se *grupa poduzetnika* definira kao poduzetnik u vladajućem položaju te njemu podređeni poduzetnici, a *obvezujuća korporativna pravila* kao postupci zaštite osobnih podataka kojih se voditelj ili izvršitelj obrade s poslovnim nastanom na području države članice pridržava tijekom prijenosa ili skupova prijenosa osobnih podataka voditelju ili izvršitelju obrade u jednoj ili više trećih zemalja unutar grupe poduzetnika ili grupe poduzeća koja se bave zajedničkom gospodarskom djelatnošću.

Cilj sklapanja obvezujućih korporativnih pravila je održati jednaku razinu sigurnosti prilikom prekograničnog i međunarodnog prijenosa osobnih podataka te osigurati jednak standard postupanja s osobnim podatcima od strane svakog poduzetnika ili poduzeća unutar grupe poduzetnika kao i od strane njihovih zaposlenika. GDPR uredba propisuje nužan sadržaj obvezujućih korporativnih pravila te ih grupa poduzetnika ili poduzeća ne može donijeti samostalno, već pravila mogu biti usvojena tek nakon što njihov nacrt odobre nadležna nadzorna tijela. Kad je riječ o grupi koja djeluje u više država, nadležna tijela svih tih država imaju utjecaj na donošenje Odluke o odobravanju obvezujućih korporativnih pravila, a glavnu riječ ima vodeće nadležno tijelo. Vodeće nadležno tijelo je tijelo države u kojoj grupa poduzetnika ili poduzeća ima glavni poslovni nastan, što će najčešće biti tijelo države u kojoj je glavno sjedište grupacije ili gdje se donosi većina odluka vezanih uz obradu osobnih podataka.

Grupa poduzetnika ili poduzeća vodećem nadležnom tijelu dostavlja nacrt obvezujućih korporativnih pravila zajedno s popratnom dokumentacijom. Vodeće nadležno tijelo donosi nacrt Odluke o prihvaćanju ili odbijanju nacrta obvezujućih korporativnih pravila koju prosljeđuje nadležnim tijelima drugih zemalja. Ako nadležna tijela ne mogu postići suglasnost o konačnoj odluci, za njeno donošenje je nadležan Europski odbor za zaštitu podataka.

3.5. Odstupanja za posebne situacije *(Smjernice na 2016/679 18/EN WP262)*

U nedostatku Odluke o primjerenosti ili odgovarajućih zaštitnih mjera, što uključuje i obvezujuća korporativna pravila, GDPR uredba pruža okolnosti u kojima se osobni podaci mogu prenijeti u treću zemlju ili međunarodnu organizaciju uz poštivanje barem jednog od sedam uvjeta:

- izričit pristanak, gdje je ispitanik obaviješten o potencijalnim rizicima takvog prijenosa
- prijenos je nužan za izvršenje ugovora, ili provedbu predugovornih mjera na zahtjev ispitanika, između ispitanika i voditelja
- prijenos je nužan radi sklapanja ili izvršenja Ugovora sklopljenog u interesu ispitanika između voditelja obrade i druge fizičke ili pravne osobe
- prijenos je nužan radi zaštite vitalnih interesa ispitanika ili drugih osoba ukoliko ispitanik fizički ili pravno nije u mogućnosti dati privolu
- prijenos je nužan iz važnih razloga od javnog interesa
- prijenos je nužan radi utvrđivanja, ostvarivanja ili branjenje pravnih zahtjeva
- prijenos se obavlja iz javnog registra koji je namijenjen pružanju informacija javnosti i gdje su ispunjeni posebni uvjeti

Ukoliko se na prijenos osobnih podataka u treće zemlje ili međunarodne organizacije ne može primijeniti nijedno odstupanje za posebne situacije, a iste ne podliježu odgovarajućim zaštitnim mjerama uključujući obvezujuća korporativna pravila, te istovremeno ne postoji Odluka o primjerenosti, prijenos je moguće ostvariti isključivo u slučaju kada se on ne ponavlja, odnosno ako se odnosi samo na ograničen broj ispitanika i nužan je za potrebe uvjerljivih,

legitimnih interesa voditelja obrade koji nisu podređeni interesima, pravima i slobodama ispitanika, a voditelj obrade je pritom procijenio sve okolnosti prijenosa podataka, na temelju čega je predvidio odgovarajuće zaštitne mjere u pogledu zaštite istih. Voditelj obrade o takvom prijenosu mora obavijestiti nadzorno tijelo i ispitanika navodeći uvjerljive legitimne interese na koje se oslanja. Prije takvog prijenosa voditelj obrade također mora procijeniti okolnosti prijenosa i pružiti odgovarajuće mjere zaštite osobnih podataka. Nadalje, kod prijenosa osobnih podataka trećim zemljama ili međunarodnim organizacijama bitno je, uz odredbe propisane GDPR uredbom o takvim postupcima, uzeti u obzir Odluku koju donosi nadzorno tijelo sukladno svojim ovlastima, uz ranije usklađivanje iste s vodećim nadzornim tijelom o uspostavi i javnoj objavi popisa vrsta postupaka obrade koji podliježu zahtjevu za procjenu učinka na zaštitu podataka. Primarno, prije bilo kakvog prijenosa osobnih podataka u treće zemlje, identično kao i prilikom uvođenja novog postupka obrade ili tehnologije obrade, voditelj ili izvršitelj obrade mora razmotriti rizike ugroze slobode ispitanika u smislu zaštite osobnih podataka. U prvom koraku potrebno je sagledavanje potrebe za provođenjem procjene učinka na zaštitu podataka. Ukoliko se utvrdi potreba za procjenom učinka na zaštitu podataka, kroz proces procjene će se utvrditi opseg podataka potrebnih za prethodnu konzultaciju s nadležnim nadzornim tijelom. Tek po primanju pozitivnog mišljenja nadležnog nadzornog tijela, voditelj obrade će pristupiti prijenosu osobnih podataka ispitanika u treću zemlju.

4. PROCJENA UČINKA NA ZAŠTITU PODATAKA PRILIKOM MEĐUNARODNOG PRIJENOSA OSOBNIH PODATAKA

Voditelj ili izvršitelj obrade s poslovnim nastanom u Europskoj uniji koji za potrebe poslovanja provodi prijenos osobnih podataka u države izvan Europskog gospodarskog pojasa mora osigurati vršenje prijenosa osobnih podataka po jednom od principa predviđenih GDPR uredbom. Kako bi se utvrdila sukladnost prijenosa s odredbama GDPR uredbe, poduzetnik mora izvršiti evaluaciju nužnosti provođenja procjene učinka na zaštitu podataka (u daljem tekstu: „DPIA“) te u slučaju potrebe prethodnu konzultaciju s nadležnim tijelom kako bi utvrdio eksponiranost riziku povrede osobnih podataka zbog nepridržavanja relevantnih odredbi GDPR uredbe. Sama procjena učinka na zaštitu nije obvezna za svaki postupak obrade, već samo za one postupke gdje postoji vjerojatnost nastanka visokog rizika za prava i slobode pojedinca. Nadležno nadzorno tijelo donosi, pored slučajeva predviđenih člankom 35., stavkom 3. GDPR

uredbe, popis vrsta postupaka obrade za koje je obvezna procjena učinka. Sam postupak procjene učinka, ukoliko ga je potrebno provesti, vrši se u suradnji s nadležnim nadzornim ili vodećim nadzornim tijelom ukoliko se radi o grupi poduzetnika s poslovnim nastanom u više od jedne države članice. Dijagram toka izrade procjene učinka na zaštitu podataka u Prilogu 2. prikazuje tri ključne faze u procjeni rizika:

(a) procjenu nužnosti provođenja DPIA
(b) provođenje DPIA
(c) provođenje prethodne konzultacije

U prvoj fazi poduzetnik utvrđuje samu potrebu provođenja DPIA kreirajući scenarij koji opisuje budući poslovni događaj. Sam scenarij mora sadržavati obilježja rizika, odnosno mora biti identificiran, analiziran i procijenjen. Nakon što se utvrde elementi budućeg poslovnog događaja, te se utvrdi postojanje vjerojatnosti visokog rizika prema odredbama iz Članka 35., stavak 3. i stavak 4. GDPR uredbe, odnosno u drugim okolnostima koje mogu dovesti do vjerojatnosti visokog rizika, poduzetnik pristupa drugoj fazi postupka, odnosno samom provođenju postupka DPIA.

U ovoj fazi poduzetnik će na osnovu scenarija budućeg poslovnog događaja utvrditi postoji li već DPIA koja opisuje navedeni budući poslovni događaj. Ukoliko postoji, poduzetnik je u mogućnosti sukladno Članku 35., stavku 1. GDPR uredbe iskoristiti postojeću procjenu koja se može odnositi na niz sličnih postupaka obrade slične visoke razine rizika. U tom slučaju poduzetnik će dopuniti i/ili korigirati postojeću DPIA i pohraniti ju za dalje korištenje u skladište DPIA te pristupiti provedbi poslovnog događaja.

Ukoliko se radi o novom budućem poslovnom događaju koji ranije nije procijenjen, poduzetnik će pristupiti procesu procjene u minimalnom opsegu, kako je definirano u Članku 35., stavak 7. GDPR uredbe, uzimajući u obzir savjet službenika za obradu podataka, sukladno odobrenom kodeksu ponašanja, te po potrebi tražiti od ispitanika ili njihovih predstavnika mišljenje o namjeravanoj obradi. Na osnovi tako provedene procjene, ukoliko DPIA i dalje indicira postojanje visokih rizika, a potreba revizije mjera za smanjenje rizika ne rezultira pozitivnim ishodom, u postupak treba uključiti nadležno nadzorno tijelo. Poduzetnik će, u postupku prethodne konzultacije s nadležnim nadzornim tijelom sukladno članku 36. GDPR uredbe, dostaviti nadležnom nadzornom tijelu odgovarajuće odgovornosti voditelja, zajedničkih voditelja i izvršitelja uključenih u obradu, svrhe i sredstva namjeravane obrade, zaštitne mjere za zaštitu prava ispitanika te, ako je primjenjivo, podatke o službeniku za zaštitu podataka i samu

procjenu rizika. Na temelju dostavljenih podataka nadležno nadzorno tijelo donijet će Odluku o mjerama koje poduzetnik mora provesti u svrhu smanjenja vjerojatnosti nastanka visokog rizika u realizaciji budućeg poslovnog događaja.

Prijenos osobnih podataka u treće države sam po sebi predstavlja visoki rizik te je u tim slučajevima poduzetnik dužan pribaviti mišljenje nadležnog nadzornog tijela, osobito u slučaju osnovane sumnje u osiguranu odgovarajuće uređenu odnosno adekvatnu razinu zaštite.

5. POSTUPANJA U SLUČAJEVIMA POVREDE OSOBNIH PODATAKA

Pojam *povreda osobnih podataka* odnosi se na : „kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani“ (GDPR uredba, članak 2., stavak 12). Sukladno tome, povreda osobnih podataka je vrsta sigurnosnog incidenta na koji se primjenjuju odredbe GDPR uredbe. Prema mišljenju 03/2014 radne skupine za zaštitu podataka iz članka 29. (dalje u tekstu: „WP29“) povreda osobnih podataka može se podijeliti u tri kategorije:

- povreda povjerljivosti- kada se povreda osobnih podataka odnosi na neovlašteno ili slučajno objavljivanje ili pristup osobnim podatcima
- povreda integriteta – kada se povreda osobnih podataka odnosi na neovlaštenu ili slučajnu izmjenu osobnih podataka
- povreda dostupnosti – kada se povreda osobnih podataka odnosi na neovlašten ili slučajan gubitak pristupa osobnim podatcima

Ovisno o okolnostima nastanka povrede osobnih podataka, ona može u pojedinačnom incidentu obuhvatiti jednu od navedenih kategorija ili više njih.

Povreda osobnih podataka može potencijalno prouzročiti štetu pojedincu, a prema GDPR uredbi to može uključivati gubitak kontrole nad osobnim podacima, ograničavanje prava pojedinca, diskriminaciju, krađu identiteta, financijski gubitak, neovlašteno dekodiranje kodiranih podataka, narušavanje reputacije, te prouzročiti i značajne ekonomske i socijalne posljedice za pojedinca.

Prema zahtjevima koje GDPR uredba postavlja ispred voditelja obrade osobnih podataka je obaveza da bez nepotrebnog odlaganja, gdje je to moguće, unutar 72 sata od saznanja o povredi zaštite osobnih podataka o istome obavijesti predmetno nadležno tijelo te u određenim slučajevima obavijesti pojedinca, osim ukoliko povreda neće rezultirati rizikom za pojedinca. Unutar tog razdoblja voditelj obrade mora procijeniti utjecaj povrede osobnih podataka na pojedinca i donijeti odluku o potrebi obavještavanja predmetnog nadležnog tijela o incidentu. Ukoliko voditelj obrade procjeni kako će povreda zaštite osobnih podataka potencijalno ili definitivno predstavljati rizik za pojedinca, potrebno je pristupiti prijavi povrede zaštite osobnih podataka nadležnom nadzornom tijelu. Voditelj obrade svoju odluku o prijavljivanju povrede zaštite osobnih podataka može temeljiti na već ranije provedenoj procjeni učinka na zaštitu podataka (DPIA) ili na konkretnom događaju. U svakom slučaju bitno je da se u trenutku identificiranja povrede zaštite osobnih podataka pokrenu mehanizmi predviđeni u Planu upravljanja incidentima.

Prijava nadzornom tijelu (*WP 250, rev.01*), mora sadržavati minimalno:

(a) opis ili prirodu povrede zaštite osobnih podataka, ako je moguće uključujući kategorije i približan broj predmetnih ispitanika te kategorije i približan broj predmetnih evidencija osobnih podataka
(b) ime i podatke za kontakt službenika za zaštitu podataka ili druge osobe za kontakt od koje se mogu dobiti dodatne informacije
(c) opis vjerojatne posljedice povrede zaštite podataka
(d) opis mjera koje je voditelj obrade poduzeo ili predložio poduzeti u cilju rješavanja problema povrede zaštite osobnih podataka, uključujući moguće mjere umanjivanja mogućih štetnih posljedica povrede

U slučajevima kada do povrede zaštite osobnih podataka dođe u procesima obrade koji obuhvaćaju prekogranični prijenos osobnih podataka (u državama unutar europskog gospodarskog pojasa), bez obzira na mjesto nastanka povrede osobnih podataka, ukoliko je procijenjeno kako treba izvijestiti nadzorno tijelo, voditelj obrade vrši prijavu vodećem nadzornom tijelu, iako do povrede osobnih podataka nije nužno došlo u državi članici pod njegovom izravnom nadležnošću.

Kada voditelj ili izvršitelj obrade nema poslovni nastan ni u jednoj članici Europske unije, a na njega se primjenjuju teritorijalne odredbe GDPR uredbe sukladno članku 3., stavak 2., isti je

dužan provesti identične procedure prijave povrede zaštite osobnih podataka kao i voditelj s poslovnim nastanom u Europskoj uniji. Za takve prijave nadležno je nadzorno tijelo države poslovnog nastana predstavnika u Europskoj uniji kojeg je voditelj ili izvršitelj obrade s poslovnim nastanom izvan Europske unije imenovao pismenim putem sukladno Članku 27. GDPR uredbe.

Uz obavezu prijave povrede zaštite osobnih podataka nadzornom tijelu, voditelj obrade u nekim slučajevima mora o povredi obavijestiti i pojedinca čiji su osobni podaci obuhvaćeni incidentom.

Obavijest pojedincu (*WP 250, rev.01*) treba sadržavati minimalno:

(a) opis prirode povrede osobnih podataka
(b) ime i prezime i podatke za kontakt službenika za zaštitu podataka
(c) opis mogućih posljedica povrede zaštite osobnih podataka
(d) opis mjera koje su poduzete ili su predložene za rješavanje problema povrede zaštite osobnih podataka, uključujući i moguće mjere umanjenja njenih mogućih štetnih posljedica

Za propuštanje obavještavanja nadzornog tijela na predviđeni način propisane su upravne kazne koje uvelike ovise o prirodi kršenja, a uključuju do 10.000.000 EUR ili, za poduzetnika, do 2% godišnjeg prometa na svjetskoj razini.

Nadalje, osoba koja je pretrpjela materijalnu ili nematerijalnu štetu zbog kršenja odredbi GDPR uredbe ima pravo naknade za pretrpljenu štetu. Iako u nekim okolnostima za štetu odgovara izvršitelj obrade, generalno se odgovornim za naknadu štete smatra voditelj obrade.

6. ZAKLJUČAK

GDPR uredba o zaštiti pojedinca u pitanjima obrade osobnih podataka te o slobodnom kretanju takvih podataka, s političkog stanovišta značajan je doprinos tekovinama ljudskih prava u Europskoj uniji. Međutim, GDPR uredba svojom širokom primjenom i uspostavljenim mehanizmima, a osobito visokim propisanim kaznenim odredbama, predstavlja značajan poslovni rizik sudionicima gospodarskih aktivnosti. Po mnogim autorima, europski pristup

zaštiti osobnih podataka je jedan od najopsežnijih i najrestriktivnijih u svijetu. Iz tih razloga nužna je široka i temeljita interdisciplinarna analiza svih poslovnih procesa u društvu te kreiranje politika i procedura koje dokumentiraju poslovne procese obrade osobnih podataka i sučeljavaju ih s odgovarajućim odredbama GDPR uredbe.

U okruženju snažne globalizacije poslovanja i podizanja konkurentnosti kroz individualizirani pristup i opsežnu analitiku kupovnih navika građana, odredbe GDPR uredbe nameću visoke standarde i načelno zabranjuju prijenos osobnih podataka izvan Europskog gospodarskog pojasa te u tom kontekstu koče slobodu poslovanja. Ipak, EK je kroz GDPR uredbu predvidjela alate koji omogućavaju globalnim poduzećima prijenos takvih podataka izvan Europskog gospodarskog pojasa u svrhu dalje obrade i analize, ali uz pridržavanje strogih propisa koji osiguravaju građanima Europske unije istu razinu prava na zaštitu osobnih podataka kakav imaju i unutar Europske unije.

Ova činjenica posebno dolazi do izražaja u slučajevima povrede osobnih podataka kada su ispred voditelja ili izvršitelja obrade postavljene obveze o stvaranju kontroliranog okvira prijenosa prava koja pojedinac ima u Europskoj uniji i na treće države gdje je došlo do povrede, te stvaranja preduvjeta pravne pomoći na koju se pojedinac čija su prava narušena može osloniti, a koje proizlaze iz odredbi GDPR uredbe.

U širem smislu, usklađivanje s odredbama GDPR uredbe daje organizacijama jezgru daljeg sagledavanja poslovnih rizika koji utječu na njihov rad, odnosno koji mogu značajno utjecati na njihovo poslovanje. Usklađivanje s odredbama GDPR uredbe predstavlja i priliku organizacijama za poboljšanja u poslovanju, dok je za voditelje obrade to prilika za uspostavljanje dubljeg povjerenja među kupcima ili korisnicima njihovih usluga, a za izvršitelje obrade usklađenje s odredbama GDPR uredbe znači diferenciranje i ukazivanje na činjenicu kako su voditelji obrade izabrali pouzdanog partnera za buduće obrade.

POPIS LITERATURE

- Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, 8. studenoga 2001., URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680080626, [pristup: 30.10.2018]

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28. siječnja 1981., URL: https://rm.coe.int/1680078b37, [pristup: 30.10.2018.]

- Direktiva 95/46/EZ Europskog parlamenta i vijeća, 24. listopad 1995., URL: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A31995L0046 [pristup: 21.08.2018.]

- Europska komisija, Komunikacija komisije Europskom parlamentu i vijeću: Razmjena i zaštita osobnih podataka u globaliziranom svijetu, 10.01.2017., URL: https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX:52017DC0007, [pristup: 10.10.2018.]

- (Europska) Konvencija za zaštitu ljudskih prava i temeljnih sloboda-pročišćeni tekst, URL: https://www.zakon.hr/z/364/(Europska)-Konvencija-za-za%C5%A1titu-ljudskih-prava-i-temeljnih-sloboda, [pristup: 17.08.2018.]

- GDPR 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 95/46/EZ (GDPR uredba o zaštiti podataka) (Tekst značajan za EGP), URL: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016R0679&qid=1538204827598&from=HR, [pristup: 01.08.2018.]

- Guidlines on Article 49 of regulation 2016/679 18/EN WP262 od 6. veljače 2018, članak 29. Data Protection working party, URL: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49846, [pristup: 01.10.2018.]

- Odluka Komisije od 5. veljače 2010. o standardnim ugovornim klauzulama za prijenos osobnih podataka obrađivačima u trećim zemljama u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća, URL: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en [pristup: 21.08.2018.]

- Odluka Komisije od 15. lipnja 2001. o standardnim ugovornim klauzulama za prijenos osobnih podataka u treće zemlje, u skladu s Direktivom 95/46/EZ i Odluka Komisije od 27. prosinca 2004.o izmjeni Odluke 2001/497/EZ u pogledu uvođenja alternativnog skupa standardnih ugovornih klauzula za prijenos osobnih podataka u treće zemlje, URL: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en [pristup: 21.08.2018.]

- Opća deklaracija o ljudskim pravima, usvojena i proglašena na Općoj skupštini Ujedinjenih naroda rezolucijom br. 217 /III 10. prosinca 1948. godine, URL: http://www.pariter.hr/wp-content/uploads/2014/10/opca_deklaracija_o_ljudskim-pravima.pdf, [pristup: 18.08.2018.]

- Povelja Europske unije o temeljnim pravima, (2016/C 202/02), URL: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:12016P/TXT&from=HR, [pristup: 01.08.2018.]

- Presuda Suda Europske unije od 6.10.2015. godine u predmetu C362/14: M.Scherms protiv Data Protection Commissioner, točke 73., 74. i 96., URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 [pristup: 10.10.2018.]

- Smjernice o obavješćivanju o povredi osobnih podataka na temelju GDPR uredbe 2016/679, WP 250 rev.01, revidirano 6. veljače 2018., URL: http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=54205 [pristup: 29.09.2018.]

- TeachPrivacy LLC, URL: https://teachprivacy.com/gdpr-whiteboard/, [pristup: 08.09.2018.]

- Ured za publikacije Europske unije, 2014, Priručnik o europskom zakonodavstvu o zaštititi podataka, URL: https://azop.hr/images/dokumenti/168/handbook_data_protection_hrv.pdf [pristup: 15.10.2018.]

- Willis Towers Watson Ltd., URL: http://intranet.willistowerswatson.com/wtwIntranetPolicies/DPIA-Template.docx, [pristup: 04.11.2018.]

- Zakon o dopunama Zakona o zaštiti osobnih podataka („Narodne novine“, br. 118/06.), URL: https://narodne-novine.nn.hr/clanci/sluzbeni/2006_11_118_2616.html [pristup: 10.10.2018.]

- Zakon o izmjenama i dopunama Zakona o zaštiti osobnih podataka („Narodne novine“, br. 41/08.), URL: https://narodne-novine.nn.hr/clanci/sluzbeni/2008_04_41_1381.html [pristup: 10.10.2018.]

- Zakon o izmjenama i dopunama Zakona o zaštiti osobnih podataka („Narodne novine“, br. 130/11.), URL: https://narodne-novine.nn.hr/clanci/sluzbeni/2011_11_130_2608.html [pristup: 10.10.2018.]

- Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i dodatnog protokola uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka („Narodne novine“, br. 4/05.), URL: https://narodne-novine.nn.hr/clanci/medunarodni/2005_05_4_38.html [pristup: 10.10.2018.]

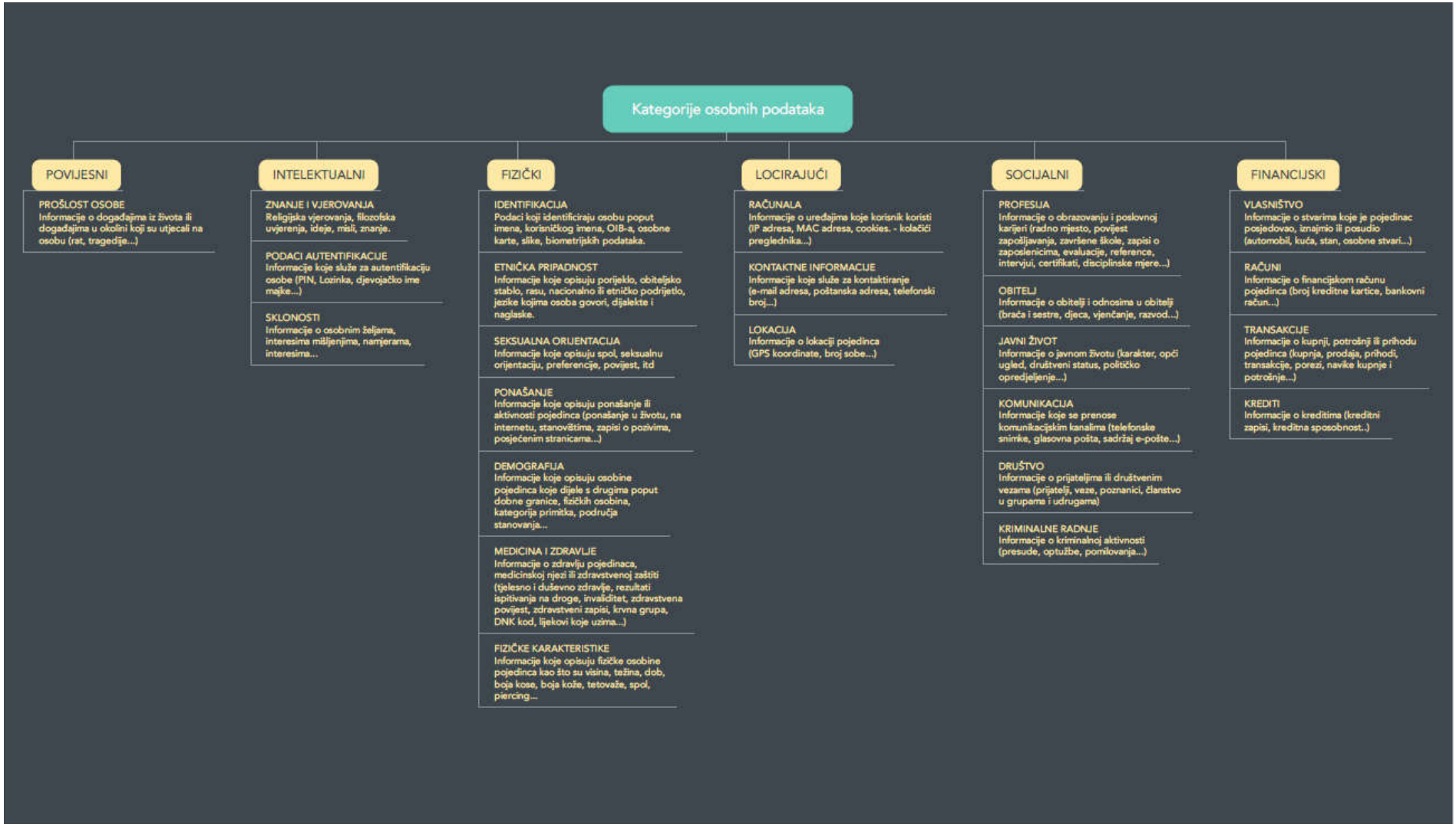
- Zakon o provedbi Opće uredbe o zaštiti podataka („Narodne novine“, br. 42/2018), URL: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html [pristup: 02.08.2018.]

- Zakonom o zaštiti osobnih podataka („Narodne novine“, br. 103/03), URL: https://narodne-novine.nn.hr/clanci/sluzbeni/2003_06_103_1364.html [pristup: 02.08.2018.]

POPIS GRAFIKONA

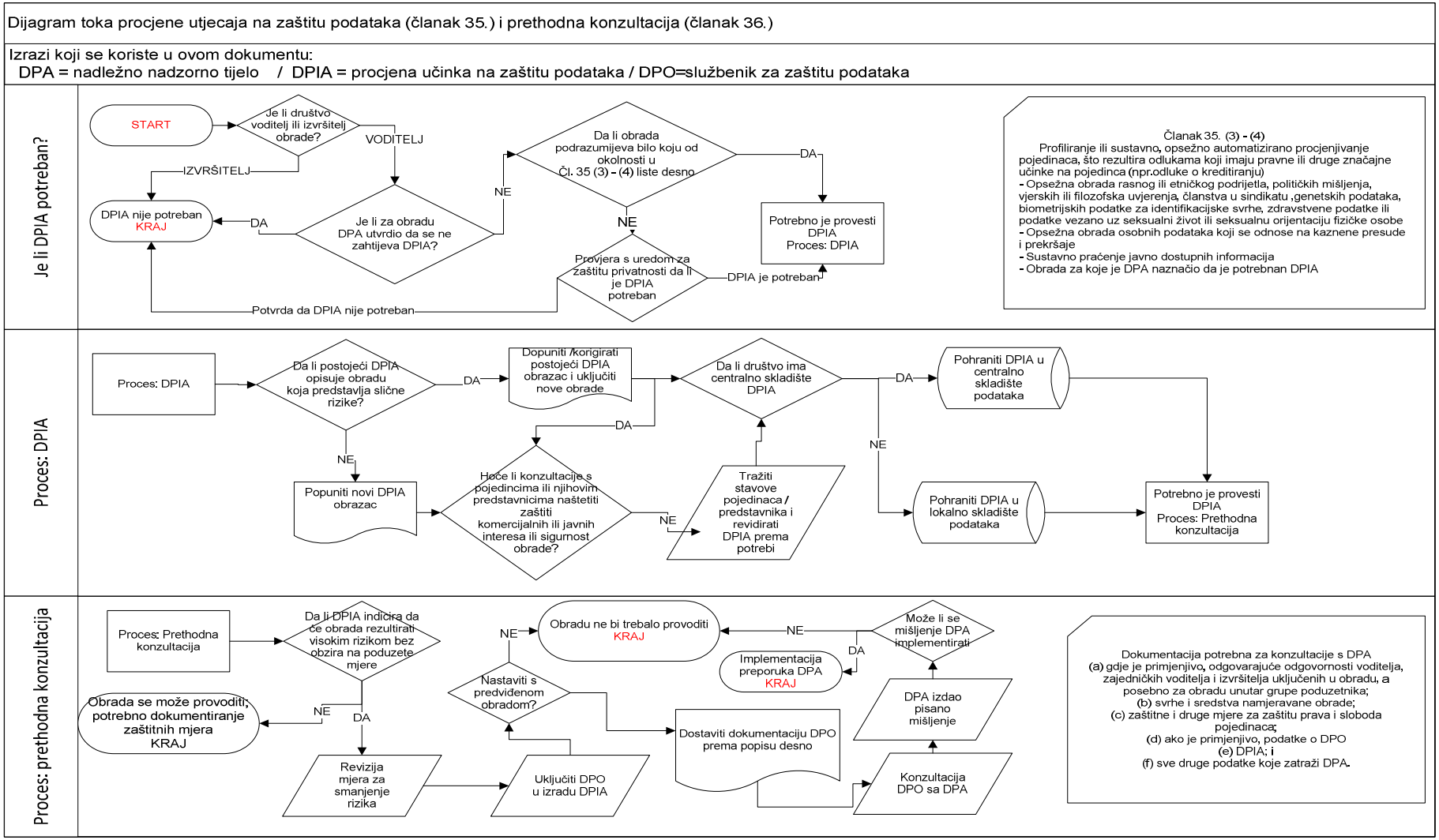
PRILOZI

PRILOG 1: Kategorije osobnih podataka



Izvor: https://xiphos.hr/gdpr-besplatni-materijali, Preuzeto: 5.9.2018, XIPHOS d.o.o.

PRILOG 2: Dijagram toka procjene utjecaja na zaštitu podataka



Izvor: Sistematizacija autora (2018)

PRILOG 3: Predložak procjene utjecaja na zaštitu podataka (DPIA)

DATA PRIVACY IMPACT ASSESSMENT TEMPLATE

The GDPR introduces a new obligation to do a DPIA (data privacy impact assessment) before carrying out any processing likely to result in high risk to individuals' interests. A DPIA is used to help identify and minimise / reduce the data privacy risks of a project/ change activity involving personal data. Here is the structure of the DPIA Process:

DPIA Template Parts		Purpose of template section	Completed by
Part 1	**Trigger Questions**	Identifies if a DPIA is required	The entity owning, initiating or designing the processing activity. If the decision is taken not to proceed with a DPIA after Stage 2 this must be confirmed with the Global Privacy Office.
Part 2	**Fact Finding Questionnaire**	Captures particulars of the activity for full DPIA.	The entity owning, initiating or designing the processing activity.
Part 3	**DPIA**	Articulation of privacy risks and mitigating actions.	The Global Privacy Office.
Part 4	**Actions & Next Steps**	Log of business actions and owners arising from DPIA.	The Global Privacy Office in conjunction with the entity owning, initiating or designing the processing activity.

DESCRIPTION OF LINE OF BUSINESS/CORPORATE FUNCTION	
WILL YOU BE A CONTROLLER OR PROCESSOR FOR ENVISIONED PROCESSING ACTIVITY?	
NAME OF INDIVIDUAL(S) COMPLETING THIS QUESTIONNAIRE	
DATE QUESTIONNAIRE COMPLETED	
DATE OF PRIOR QUESTIONNAIRE COMPLETION (IF APPLICABLE)	
DESCRIPTION OF PROCESSING ACTIVITY	
INFORMATION REGARDING DESIRED TIMELINE BEFORE ACTIVITY IS LIVE/IS ACTIVITY ALREADY LIVE	

PART 1 – TRIGGER QUESTIONS

Primary Trigger Questions
Please indicate (by clicking 'Yes' or 'No') whether the change activity/ proposed process involves, or could potentially involve:

	Question	Yes/ No	Guidance/ Considerations:
1	**Does this activity involve the processing of personal data?**	☐ Yes ☐ No	Personal data means data which relates to a living individual who can be identified by any of the following: (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, (c) includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. *Examples:* • Name • Address • Phone numbers • Bank details • DOB • National insurance number
2	**Does this activity involve the processing of sensitive personal data?**	☐ Yes ☐ No	*Examples:* • Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or sexual orientation. • Alleged or proven criminal offences. • Genetic data, biometric data, physical or mental health.

If you have answered '<u>Yes</u>' to questions 1 OR 2, please move onto the 'Secondary Trigger Questions'.

If you have answered '<u>No</u> to both, you are not required to carry out a DPIA.

	Secondary Trigger Questions: *Please select 'Yes' or 'No'.*		
	Question	**Yes/ No**	**Guidance/ Consider:**
3	**Will the project involve the collection of new information about individuals?**	☐ Yes ☐ No	- *What data will be collected in addition to existing data?*
4	**Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?**	☐ Yes ☐ No	- *What individuals/ organisation now has access to the data?* - *What data do they have access too?* - *Why do they need access?*
5	**Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?**	☐ Yes ☐ No	- *Is there a legitimate reason for using this data?*
6	**Will the project/ change result in you making decisions or taking action against individuals in ways which could have a significant impact on them?**	☐ Yes ☐ No	- *What impact will this have on the individual?* - *Is this necessary?*
7	**Will the project involve processing of information about children under 16?**	☐ Yes ☐ No	- *What procedures will be in place to ensure that children fully understand how their personal data will be processed?* - *Will consent from children's parents/guardians be obtained for the processing of children's data?* - *What procedures are in place to verify parental consent and/or the child's age?* - *Does the change activity involve profiling, making wholly automated decision, or using biometric data in relation to children?*
8	**Will the project make use of cloud technology?**	☐ Yes ☐ No	- *Consider whether the cloud is public/ private/ community/ hybrid* - *Is there a contract in place with the cloud service provider?* - *Is the cloud service provider based within the EEA/are its servers hosted within the EEA?* - *Does the cloud service provider use sub-contractors or affiliates? If so, where are they based and is there consent?* - *Will data be encrypted in transit to the cloud service provider?*
9	**Will the project use automated decision making/ profiling?**	☐ Yes ☐ No	- *Is there any human involvement in the automated decision-making process, e.g. human checks at any stage of the decision?* - *If decisions are wholly automated, will consent be obtained from individuals to make the automated decision? How will individuals be able to withdraw their consent and how will you ensure that wholly automated decisions do not take place if consent is withdrawn?* - *Is the wholly automated decision necessary in*

			connection with a contract between WTW's and the relevant individual?
10	**Will the project compel individuals to provide information about themselves?**	☐ Yes ☐ No	- *Will the project/ change activity require individuals to provide personal data?*
11	**Will data be stored/ processed/ transferred outside of the EEA?**	☐ Yes ☐ No	- *Where is the data stored, how it is stored, how is it processed?*
12	**Will the project require you to contact individuals in ways that they may find intrusive?**	☐ Yes ☐ No	- *Consider how and why you are contacting individuals.* - *Has consent been obtained?* - *Is there a legitimate reason to contact the individual?*
13	**Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations?**	☐ Yes ☐ No	- *For example, health records, criminal records or other information that people would consider to be private.*

If you have answered "<u>Yes</u>" to any of the secondary questions, please move on to "<u>Part 2</u>".

If you have answered "<u>No</u>" to all of the questions, please consult with the Global Privacy Office to verify if a DPIA is not needed. The reason for not performing a DPIA must be recorded.

PART 2 – FACT FINDING QUESTIONNAIRE

Please address the following questions as comprehensively as possible so that we can carry out a Privacy Impact Assessment of the proposed project and provide recommendations aimed at facilitating the project through the adoption of suitable privacy practices.

1.	2. QUESTIONS	3. PLEASE COMPLETE THIS COLUMN
	Project name	*Please enter the name of the project as it can be referred to throughout.*
	Willis Towers Watson entity ("WTW Entity")	*Please enter the name of the legal entity that will carry out the project*
	Brief description of the project	*Please enter a description of the proposed technology which the WTW Entity intends to use, how it works, whether any external companies are providing any services, the reasons for its implementation, and a description of how this will change any WTW operations.* *This could include, for example, a brief description of how individuals will interact with the project e.g. if it establishes a client-facing platform, or alternatively that there will be no client-facing element.*
	Your name and contact details	*The name and contact details (email address and telephone number) of the person completing this form.*
	Section A: Geographical impact of the project	
	Is any EU-based entity involved in the project?	**YES** **NO** Please provide details of the entity/entities involved in the processing and its geographic location: *In each case, please provide the full legal name of the entity and the country in which it is located.* *Where non-EU entities are involved, please also include a list of countries where those entities are located*
	Does the project affect EU-based individuals?	**YES** **NO** If YES, please list the EU countries where the individuals are based: *Please list the EU countries where the individuals who will be affected by the project live.* *It is not necessary to list the individuals who live in non-EU countries*
	Section B: Nature of the data	
	Will the project involve the collection, use or disclosure of "personal data"?	**YES** **NO** If YES, please identify the main types of personal data collected, used or disclosed:

		If NO, please explain the types of non-personal data which are collected, used or disclosed. *1) Please provide a list of all categories of data collected, used and disclosed by the WTW Entity. Please note that the definition of personal data is very broad (it incorporates all data and similar data set out in the examples below). This can either be data which has been explicitly provided by the individual to the WTW Entity, or can also be data which is collected by the WTW Entity from other entities, or even data which is collected by the WTW Entity automatically via cookies or other device identifiers.* *Examples* *Data actively provided by individuals: first name, last name, email address, telephone number, marital status.* *Data obtained by the WTW Entity from other entities: data purchased from data brokers including the sorts of behavioural data described below* *Data collected automatically: individual identifiers such as an IP address, MAC address, cookie identifier, or any information collected which could be linked to any of these unique identifiers. Including individual clicks which an individual makes on a website and the length of time an individual spends on a particular web page.* *2) Please also provide details of whether this constitutes a change to the amount or types of data collected by the WTW Entity, in comparison to the types of data it has collected up to now.*
	Will the project involve the collection, use or disclosure of "sensitive personal data"?	**YES** **NO** If YES, please provide details: *Sensitive personal data includes: information relating to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, genetic, health and sex life.* *Please also include details of where the project involves the processing of criminal convictions or other criminal offences.* *If any of these categories of data are collected as part of the project, these should be listed here*
	Does the project involve data accessed from, or stored in, an individual's device? For example, retrieving a MAC address from an individual's mobile phone or storing cookies on an individual's computer.	**YES** **NO** If YES, please provide details: *If, to collect data for the project, the WTW Entity will scan and collect information which is emitted from a device (such as a MAC address, which a device uses to assist with connecting to local wifi networks), please provide details of this here.* *Furthermore, if the WTW Entity will store information on a user's device (for example a cookie being stored on a user's computer to ensure that their login details are remembered) then please provide details of each individual cookie or other identifier here.*

	Section C: Responsibility for data usage	
	Who is the "owner" of the data used in the context of this project?	Please explain your response and provide details of the relevant entities and / or clients: *Please describe the entity which is responsible for collecting that data, will be responsible for ensuring its accuracy, and would have the right to sell or licence that data on (if it were permitted by applicable laws).* *Please also set out which entities will have access to and will also be able to make choices about what the data will be used for. For example, will the WTW Entity be able to aggregate all client data for analytics purposes?*
	Who is responsible for making decisions about the collection, use, storage and / or disclosure of data in the context of this project?	Please explain your response and provide details of the role of the WTW Entity and /or the client in relation to this decision-making: *Please set out the entity which collects the categories of data and makes choices about what the data will be used for. For example, in respect of employees, the 'owner' could be the employing WTW Entity. In relation to particular clients, the 'owner' of the data could be the local entity which that client contracts with.*
	Section D: Compliance standards	
	Transparency	
	Are you aware of any steps taken to notify a data protection authority about the data processing activities relevant to this project?	**YES** **NO** If YES, please provide details: *Each EU country has a data protection authority. Under the GDPR, there are certain circumstances in which the data protection authorities should be informed of the processing activities, particularly where the uses of data will be particularly intrusive to the privacy rights of individuals. Please set out if the proposed project has been notified to or discussed with any data protection authority.*
	Will a data protection statement or privacy policy be used for the purpose of informing individuals of the uses and disclosures made of their data?	**YES** **NO** If YES, please provide details and/or link: *Please explain whether there is an existing privacy policy which is intended to provide notice of the proposed uses of personal data, or if a separate notice will be provided to individuals. Please provide a link or an attached copy in each case.*
	Legitimacy	
	Will the WTW Entity (or the client, if relevant) seek consent from individuals to use their data in the context of this project?	**YES** **NO** If YES, please provide details: *If YES, please describe which uses for individuals' data*

		the WTW Entity obtains consent in relation to. *Please also explain when consent will be obtained from individuals, how it will be obtained (for example if it is obtained by clients ticking a box on a website when they sign up for an account), and where it will be recorded.*
	Will any third party that discloses data to the WTW Entity in the context of this project obtain consent from individuals in respect of the use of the data by the WTW Entity?	**YES** **NO** If YES, please provide details: *If YES, please describe which data obtained from third parties will the WTW Entity use on the basis of consent given to third parties.* *Please also explain how the WTW Entity will ensure that appropriate consent has been given by third parties. For example, the WTW Entity could obtain contractual protection from third parties, and could carry out due diligence on third parties by asking appropriate questions to ensure that appropriate consent has been obtained.*
	If the answer to the above questions regarding consent is NO, do any of the following cases apply:	The data is necessary to provide a product/service. The data is necessary to comply with a legal obligation. The data is necessary to protect individuals. The data is necessary in the public interest. The data is necessary for the WTW Entity's interests and its use does not adversely affect individuals. Please provide further details about any options selected: *We anticipate most uses of data will be carried out on the basis of the WTW Entity's legitimate interests, which must not outweigh the interests of the individuals concerned. In this case, please provide details about which of the WTW Entity's interests are being protected, and any reasons why the individuals' right to privacy is not disproportionately affected. For example, in the case of installing CCTV cameras on office premises, the legitimate interest would be the security of the WTW Entity premises and crime prevention. The WTW Entity could then explain that CCTV images are retained for only a short period of time, and that only a limited area is covered by CCTV footage.* *In the event that one of the other options will apply to the uses of personal data, please explain why this is the case.*
	Purpose limitation	
	Please describe all of the intended purposes for which data is collected, used, stored and disclosed in the context of this project. For example, for analytics purposes, for human resource management or vendor management purposes, to manage client contacts, etc.	*Please describe the purposes is a reasonable level of detail. For example, rather than simply 'analytics' or 'marketing', please use descriptions such as 'sending email marketing messages' or carrying out analytics on employee performance metrics. Other examples might be: human resource management purposes, managing employee contracts or vendor management purposes, to manage client contacts, etc.*

	Is the data shared with any other party?	**YES** **NO** If YES, please provide details of all potential recipients and the likely uses of the data made by those recipients: *Please list the categories of entities that the WTW Entity might share data with. For example, this might include service providers (where possible, list the types of services they might be providing such as human resources services or cloud storage services) or group companies.* *In relation to each of these categories of recipients, please describe what purposes the third parties may use the data for and whether they will have the rights to make choices about the purposes for which the data will be used. For example, if data will be provided to third party service providers will those providers be restricted to acting on the WTW Entity's instructions, or will they be able to use the data for other products and projects.*
	Proportionality	
	Is <u>all of the data</u> collected or used necessary for the purposes identified above?	**YES** **NO** If NO (or not entirely), please explain the reasons why the data which is not necessary for these purposes is collected: *For example, where CCTV cameras are installed on office premises, not all of that data will be used in the event that no criminal activity takes place or there is no reason to review it. The data is still collected on the basis that this is not known. In such a case, this description should be set out here.*
	Quality	
	How will data collected in relation to this project be maintained, kept accurate and up to date?	*Please explain how data will be stored. For example, will it be kept on an internal or cloud system?* *Please describe any ways in which the WTW Entity will ensure that, at the point of collection, the data collected is accurate. For example, when a user creates an account, will they be required to verify their email address (where an email is sent including a unique link to verify the address is real)?* *Please explain what functionality there will be to keep data up to date. For example, will it be possible for employees to update data fields which a client informs them that they are incorrect?*
	How long will the data be retained for? Please provide details of any periodic description / destruction of obsolete data if relevant.	*Please explain how long data will be retained by the WTW Entity. For example, this could state that employee data will be retained for as long as the individual is an employee, plus an additional two years, unless there is a reason to keep it longer.* *Please also explain how decisions on when to retain data beyond a usual period will be made: which function of the business is able to make these decisions?*

	How will data be disposed of when is no longer required?	*Please explain how data will be deleted from the WTW Entity's systems.*
	Individuals' rights	
	How will any requests from individuals be handled? For example, complaints, enquiries, requests to opt-out, not to receive marketing communications or for access to information about the data held about them?	*Please describe whether there are procedures which the WTW Entity has in place to handle requests to, for example, opt-out of marketing messages, have their data updated or deleted, access their data, object to profiling or other processing and restrict processing.*
	Data security	
	What security measures will be in place to ensure the confidentiality of data?	*Please describe the measures in place, for example what authentication procedures are in place (e.g. SSO, IP whitelisting). Are there organisational measures in place, such as restricted access based on an individual's role within the WTW Entity. Please also explain who determines the access level for each individual.*
	Will the use, collection, storage and disclosure of information in the context of this project will be subject to any of the following:	*Please describe any of the following which apply:* *Physical security measures (e.g. card access only to rooms or buildings where data can be accessed)* *An information security policy* *Controls on access to information (e.g. password protection on all information, encrypted laptops and USB drives to access personal data only)* *A business continuity plan (in the event of data loss)* *Internal training programme on security systems and procedures (e.g. data protection training. Please also describe which relevant members of staff received such training)* *Procedure to investigate breaches of security when they occur (please provide details of the principal steps in such procedure)* *A recognised standard on information security standard (e.g. ISO/IEC 27002)* *Please provide further details about any options selected:*
22.	**Will any third party vendors process data on behalf of the WTW Entity or collect data that will subsequently be used by the WTW Entity?**	**YES** **NO** If YES, please provide details of all relevant third parties and their role: *Please describe each vendor and the service they provide to the WTW Entity. For example, [vendor name]: payroll software.* *Please also attach copies of any written contract governing that relationship.*

	International data flows	
23.	**Will the WTW Entity share data with organisations based outside of Europe?** In providing your response, please also consider the locations of: ● Any servers on which the WTW Entity or vendors will process data. ● Any offices from which employees and vendor staff may remotely access servers processing data.	**YES** **NO** *If YES, please provide details of each organisation the data will be shared with an indicate:* ● *whether it is part of the WTW group of companies;* ● *its geographic location; and* ● *if there is a written contract governing the relationship.*

PART 3 – DATA PRIVACY IMPACT ASSEMENT

For each data protection principle, please note down any privacy risks to the data subject associated with the proposed activity, any applicable mitigation factors and assess the impact the risk may have on the data subject if it materialises together with an assessment on the likelihood of the risk materialising. If the activities and systematic processing operations are not sufficiently clear and adequately described in Part 2, please obtain further information from the business before completing Part 3.

Principle	**Risks - Both to Individual and to WTW**	**Mitigating Actions/ Solution**	**Risk Materialisation** (Low/Medium/High)		**Approved by** (Name of Person)
			Impact	**Likelihood**	
1: Fair, Lawful & Transparent Please record the Legal Basis for processing or legitimate purposes of data collection as applicable. Please also record whether the processing is covered by existing privacy notices or whether additional privacy notices will be required.					
2. Is consent relied on for legal basis to process? If 'Yes" please detail how it is to be collected, recorded and managed.					
3: Purpose Limitation Please cover: Necessity and proportionality by reference to the purpose(s) of processing.					

4. Data Minimisation/ Adequate Please cover: How Privacy by Design Principles are met. How is minimum access to information achieved? Is the information adequate but not excessive? Are all data fields necessary for purpose?					
5: Accuracy Please outline data rectification processes.					
6: Retention Please confirm retention period is appropriate, and how it will be adhered to, and deletion of data is possible.					
7: Data Subject Rights ☐ Access ☐ Rectification ☐ Restriction ☐ Objections ☐ Automated Decisions ☐ Portability ☐ Right to be forgotten ☐ Consent withdrawal **Please cover how data subject rights requests are to be managed**					
8: Security Please cover safeguards and security measures. Please provide					

any relevant documentation. How the risk of loss, damage or unauthorised disclosure to the personal data (or potentially other data sets) mitigated? If there are transfers to third parties, are there appropriate contracts and has appropriate due diligence been carried out? If there are joint controller issues, have all Article 26 issues been covered?					
9: International Data Transfers Are transfer mechanisms adequate for the transfers taking place?					
10: Direct Marketing If direct marketing will be carried out, please detail measures to ensure appropriate consents obtained.					
11. Cookies If the project involves setting cookies, please provide details of the measures that will be in place to ensure adequate transparency information provided and consent obtained					

PART 4 – ACTIONS & NEXT STEPS

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for a privacy concerns that may arise in the future?

Actions	Owner	Date for completion of Actions	Completed?
			☐ Yes ☐ No
			☐ Yes ☐ No
			☐ Yes ☐ No
			☐ Yes ☐ No

Completed by (Contact point for future privacy concerns):

Name:	
Date:	

Izvor: http://intranet.willistowerswatson.com/wtwIntranetPolicies/DPIA-Template.docx, Preuzeto: 4.11.2018, Willis Towers Watson Ltd.