USKLAĐIVANJE INFORMACIJSKIH SUSTAVA ORGANIZACIJE SA ZAHTJEVIMA GDPR UREDBE

Balen, Darija

VISOKO UČILIŠTE ALGEBRA

DIPLOMSKI RAD

USKLAĐIVANJE INFORMACIJSKIH SUSTAVA ORGANIZACIJE SA ZAHTJEVIMA GDPR UREDBE

Darija Balen

Zagreb, rujan 2018.

Predgovor

Zahvaljujem mentoru, mr.sc. Draženu Oreščaninu na pomoći, savjetima i smjernicama prilikom izrade diplomskog rada.

Zahvaljujem tvrtki Poslovna inteligencija d.o.o. koja je podržala i omogućila moje daljnje školovanje i bez čijeg ukazanog povjerenja danas ne bih bila dio jedne predivne zajednice.

Posebno hvala mojim roditeljima i obitelji koji su mi velika moralna podrška i koji su me naučili kako koračati kroz život.

Prilikom uvezivanja rada, Umjesto ove stranice ne zaboravite umetnuti original potvrde o prihvaćanju teme diplomskog rada kojeg ste preuzeli u studentskoj referadi

Sažetak

Najava stupanja na snagu Opće uredbe o zaštiti podataka, skraćeno GDPR, uvelike je promijenila fokus poslovanja tvrtki, u vidu zaštite osobnih podataka. Skrenuta je pozornost na osobne podatke svih građana Europske Unije, a najavljivane visoke kazne izazvale su negativnu reakciju javnosti. Tvrtke se susreću s novim načinima razumijevanja definicija osobnih podataka i svoje poslovne sustave moraju prilagoditi kako bi bile u mogućnosti ispuniti nove zahtjeve koje GDPR donosi. GDPR uvodi i nove uloge i odgovornosti u procesu obrade osobnih podataka, pa se tako susrećemo s pojmovima poput Ispitanik ili Subjekt obrade, Voditelj obrade, Izvršitelj obrade i Službenik za zaštitu podataka.

Svaka tvrtka je drugačija po pitanju poslovanja i prikupljanja osobnih podataka ispitanika, te korištenja poslovnih sustava koje je potrebno prilagoditi. Većina ranijih programskih rješenja nisu dizajnirana na način da podržavaju zahtjeve poput prava na pristup, prava na zaborav i prava na prenosivost podataka.

Ideja diplomskog rada je prikazati novitete koji dolaze stupanjem GDPR-a na snagu, te načine na koje će se tvrtke morati uskladiti kako bi bile u mogućnosti ispuniti sve zahtjeve ispitanika. Prilikom izrade rada opisala sam neka moguća rješenja usklađenja tvrtke sa zahtjevima GDPR-a, te u sklopu internog projekta u tvrtki u kojoj radim, napravila analizu stanja, rizika i plan sigurnosti podataka. Rad je pisan na način da može poslužiti kao svojevrstan vodič za implementaciju GDPR-a u bilo kojoj tvrtki.

Ključne riječi: GDPR, osobni podaci, zahtjevi, ispitanik, usklađivanje.

Summary

The announcement of the entry into force of the General Data Protection Regulation. abbreviated GDPR., has greatly changed the company's business focus, in terms of personal data protection. Attention has been paid to the personal data of all citizens of the European Union, and the announcement of high penalties caused a negative public reaction. Companies face new ways of understanding the definition of personal information and their business systems need to adapt to be able to meet the new demands that GDPR delivers. GDPR also introduces new roles and responsibilities in the processing of personal data, so we meet with terms such as the Data Subject, the Data Controller, the Data Processor, and the Data Protection Officer.

Each company is different in terms of business and collecting personal data of respondents and the use of business systems that need to be adjusted. Most of the earlier programming solutions were not designed to support requirements such as right to access, right to be forgotten, and right to data portability.

The idea of this graduate thesis is to present the novelties that come with the entry of the GDPR into force, and the ways in which companies need to be harmonized to be able to meet all the requirements of the respondents. During the work I described some possible solutions to the company's compliance with GDPR requirements and, as part of the internal project in the company I worked on, analyzed the current state, risk and data security plan. The paper is written in a way that it can serve as a guide to the implementation of GDPR in any company.

Keywords: GDPR, Personal Data, Rights, Data Subject, Harmonization.

Sadržaj

1. Uvod 1

2. Općenito o GDPR-u i privatnosti podataka 2

2.1. Povijest zaštite privatnosti podataka 2

2.2. Osobni podaci 4

2.3. Uloge i odgovornosti 5

2.4. Nadzorno tijelo 7

3. Funkcionalni zahtjevi 9

3.1. Izvješćivanje o povredi osobnih podataka 10

3.2. Pravo na pristup 11

3.3. Pravo na zaborav 12

3.4. Pravo na prenosivost podataka 13

4. Proces usklađivanja informacijskih sustava organizacije 14

4.1. Analiza stanja 15

4.1.1. Članak 30.: Evidencija aktivnosti obrade 16

4.1.2. Članak 6.: Svrha obrade osobnih podataka 20

4.2. Analiza rizika 21

4.3. Izrada plana sigurnosti podataka 26

4.4. Integracija GDPR IT rješenja 29

5. Otkrivanje osobnih podataka 30

5.1. Strukturirani elektronički podaci 30

5.2. Nestrukturirani elektronički podaci 31

5.3. Ne-elektronički podaci 33

6. Upravljanje i zaštita osobnih podataka 34

6.1. Kontrola pristupa podacima 34

6.2. Zaštita osobnih podataka na izvoru – anonimizacija podataka 35

6.3. Maskiranje podataka 38
7. Privola ispitanika 41
8. Proces upravljanja zahtjevima ispitanika 43
9. Primjer softverskog rješenja 46
10. Zaključak 48
Popis kratica 50
Popis slika 51
Popis tablica 52
Literatura 53

1. Uvod

Europski Parlament i Vijeće su dana 27. travnja 2016. godine odobrili Uredbu (EU) 2016/679 o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka). GDPR se direktno primjenjuje na sve članice Europske Unije, ali se uskladiti moraju i sve tvrtke izvan Europske Unije koje posluju s građanima Europske Unije, odnosno prikupljaju i obrađuju njihove osobne podatke. Kazne za tvrtke koje se ne budu pridržavale GDPR-a mogu iznositi do 4% godišnjeg prometa ili 20 milijuna eura, u ovisnosti što iznosi više.

Definirane su glavne uloge koje sudjeluju u procesu obrade podataka, a to su ispitanik, voditelj i izvršitelj obrade, te službenik za zaštitu podataka. Definirano je i nadzorno tijelo, čija je uloga savjetovati i rješavati probleme povreda nad osobnim podacima ispitanika. U Hrvatskoj je za tu ulogu imenovana Agencija za zaštitu osobnih podataka (skraćeno AZOP).

Veliki naglasak se stavlja na privole bez kojih, u situacijama kada ne postoji zakonska obveza, tvrtke ne smiju obrađivati osobne podatke ispitanika. Uvedena su nova prava pojedinaca koja utječu na funkcionalne zahtjeve trenutno korištenih poslovnih sustava.

U ovom radu će biti opisani noviteti koje donosi GDPR te neki od načina usklađivanja informacijskih sustava organizacije sa zahtjevima GDPR-a.

Za potrebe boljeg razumijevanja bit će kreiran primjer analize stanja tvrtke u odnosu na usklađenost s GDPR-om, analiza rizika te plan sigurnosti osobnih podataka.

Također, bit će opisana i navedena neka od postojećih rješenja na tržištu, te dane smjernice kako bi se tvrtke mogle čim bolje zaštititi i uskladiti s GDPR-om.

2. Općenito o GDPR-u i privatnosti podataka

2.1. Povijest zaštite privatnosti podataka

Od početaka korištenja elektroničkih računala za obradu podataka, države su postale svjesne opasnosti od zlouporabe korištenja novih informacijskih tehnologija. Najveći rizik predstavljala je mogućnost iznošenja velikih količina podataka o građanima izvan granica države.

Njemačka savezna država Hessen je 1970. godine donijela i usvojila prvi zakon o zaštiti osobnih podataka, poznat pod nazivom *Bundesdatenschutzgesetz* (skraćeno BDSG). Bio je to savezni zakon o zaštiti podataka koji je uređivao izlaganje osobnih podataka koji se ručno obrađuju ili pohranjuju u IT sustavima. Ubrzo nakon Njemačke, slične zakone su donijele Švedska, Francuska i Danska.

Njemački savezni Ustavni Sud je 1983. godine, za vrijeme popisivanja stanovništva, donio odluku o informacijskom samoodređenju, kojom je definirana zaštita pojedinaca od neograničenog prikupljanja, skladištenja, korištenja i otkrivanja njihovih osobnih podataka, a u kontekstu suvremene obrade podataka. Time je zajamčena sposobnost pojedinaca da odlučuju o tome koje informacije o sebi trebaju prenijeti drugima i pod kojim okolnostima.

Ugovor o zaštiti pojedinaca u pogledu automatske obrade osobnih podataka, potpisan je kao Konvencija Vijeća Europe 108 i stupio je na snagu 1. listopada 1985. godine. Ugovor je ratificiran od svih 47 članica Vijeća Europe, osim Turske.

„Kao punopravna članica Vijeća Europe, Republika Hrvatska je od ostvarenja svoje neovisnosti i samostalnosti postala stranka mnogih međunarodnih ugovora, pa tako i onih međunarodnih ugovora i instrumenata koji se odnose na ljudska prava. Konvencija o zaštiti osoba glede automatizirane obrade osobnih podataka, važan je dodatak već postojećem sustavu zaštite ljudskih prava i temeljnih sloboda, osobito prava na privatnost, koje je priznato i u članku 8. Konvencije za zaštitu ljudskih prava u poštivanju privatnog života. Temeljem konvencije o zaštiti pojedinaca pri automatskoj obradi osobnih podataka, izrađena je Direktiva Europskog Parlamenta i Vijeća Europske Zajednice 95/EZ o zaštiti pojedinaca u okviru obrade osobnih podataka, te o slobodnom tijeku tih podataka, usvojena 20. veljače 1995. godine, a kojom se osnažuju i proširuju načela zaštite prava i slobode pojedinaca, posebno pravo na privatnost. Konvencija ima za cilj zajamčiti svakoj fizičkoj osobi zaštitu

njezinih prava i temeljnih sloboda, osobito njezino pravo na zaštitu privatnosti pri automatiziranoj obradi osobnih podataka, na teritoriju svake ugovorne strane, bez obzira na njezino državljanstvo ili mjesto stanovanja.“[1]

Tijekom posljednjih 25 godina tehnologija je toliko napredovala da je promijenila načine života, a sukladno tome bilo je potrebno pregledati i urediti postojeća pravila i zakone.

U vrijeme samih početaka interneta, točnije 24. listopada 1995. godine, usvojena je Direktiva 95/46/EZ Europskog Parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (eng. *The European Data Protection Directive*).[2] U Direktivi su definirana značenja sljedećih pojmova: osobni podaci, obrada osobnih podataka, sustav arhiviranja osobnih podataka, nadzornik, obrađivač, treća stranka, primatelj i suglasnost osobe čiji se podaci obrađuju.

Europski Parlament i Vijeće su dana 27. travnja 2016. godine odobrili Uredbu (EU) 2016/679 o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka). Aktualna Uredba (EU) 2016/679 poznatija je pod engleskim nazivom *General Data Protection Regulation* ili skraćeno samo GDPR. Uredba je stupila na snagu 25. svibnja 2018. godine, a njome je prestala važiti prijašnja Direktiva 95/46/EZ, ali i odredbe lokalnih zakona, poput Zakona o zaštiti osobnih podataka (NN 103/03, 118/06, 41/08, 130/11).

GDPR se direktno primjenjuje na sve države članice Europske Unije, ali se uskladiti moraju i sve tvrtke izvan Europske Unije, koje posluju s građanima Europske Unije, odnosno prikupljaju i obrađuju njihove osobne podatke. GDPR se ne odnosi samo na tvrtke koje posluju s krajnjim korisnicima (poput telekoma, banaka, maloprodaja i sličnih), već i na tvrtke koje posluju s drugim tvrtkama, jer i one moraju poštivati regulativu za prikupljanje i obradu podataka o zaposlenicima, partnerima itd.

Iz ranije navedenoga, vidljivo je kako zaštita osobnih podataka nije nikakva novost, ali je radi sve bržeg napretka tehnologije bilo potrebno dodatno urediti postojeće zakone, osvijestiti pojedince o njihovim pravima, te još bolje zaštititi osobne podatke pojedinaca.

U zadnje vrijeme sve se češće spominje izreka koja govori kako su podaci „nafta budućnosti“ jer i podatke treba procesirati kako bi se otkrila njihova prava vrijednost. Iz dana u dan generiraju se sve veće i veće količine podataka, pogotovo dolaskom pametnih telefona, Interneta stvari, pametnih kuća, autonomnih automobila i slično. S obzirom na GDPR,

potrebne privole i jasne svrhe obrade podataka, do podataka će se u budućnosti sve teže dolaziti. Tvrtke koje raspolažu velikim količinama podataka imat će ih i dalje priliku monetizirati, a sukladno novom okruženju koje ih očekuje radi GDPR-a, kreirat će se i nove usluge i novi modeli.

2.2. Osobni podaci

Prijašnja važeća Direktiva 95/46/EZ sadržavala je samo jednu definiciju koja se odnosila na osobne podatke, a glasila je ovako:

- „osobni podaci“ znači bilo koji podaci koji se odnose na utvrđenu fizičku osobu ili fizičku osobu koju se može utvrditi („osoba čiji se podaci obrađuju“); osoba koja se može utvrditi je osoba čiji je identitet moguće utvrditi, izravno ili neizravno, a posebno navođenjem identifikacijskog broja ili jednog ili više činitelja značajnih za njegov fizički, fiziološki, mentalni, gospodarski, kulturni ili socijalni identitet;[3]

Ono što se promijenilo stupanjem GDPR-a na snagu, je donošenje novih definicija koje proširuju kontekst značenja osobnih podataka, poput sljedećih:

- „osobni podaci“ znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik“);
  pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca;
- „povreda osobnih podataka“ znači 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;
- „genetski podaci“ znači osobni podaci koji se odnose na naslijeđena ili stečena genetska obilježja pojedinca koja daju jedinstvenu informaciju o fiziologiji ili zdravlju tog pojedinca, i koji su dobiveni osobito analizom biološkog uzorka dotičnog pojedinca;

- „biometrijski podaci“ znači osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci;
- „podaci koji se odnose na zdravlje“ znači osobni podaci povezani s fizičkim ili mentalnim zdravljem pojedinca, uključujući pružanje zdravstvenih usluga, kojima se daju informacije o njegovu zdravstvenom statusu; [4]

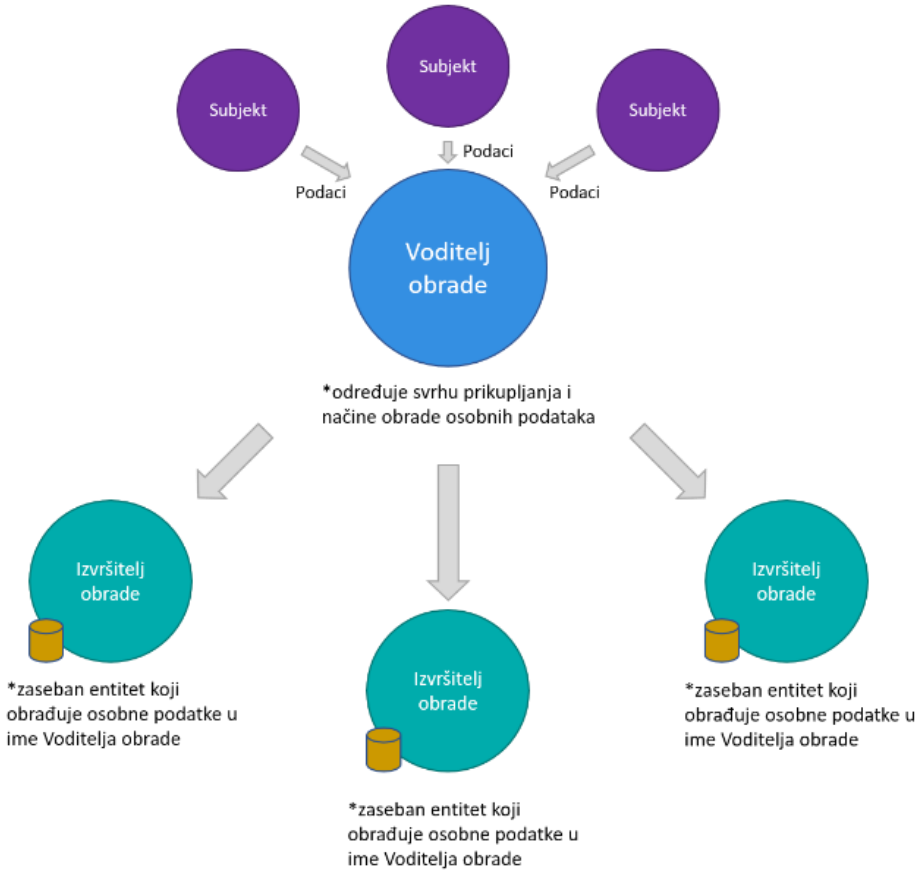
Osobni podaci su razvojem tehnologije postali mnogo više od onoga što se do sada podrazumijevalo tom definicijom. Potrebno je istaknuti kako u osobne podatke osim imena i prezimena, osobnog identifikacijskog broja (OIB), adrese i broja telefona, spadaju i adresa elektroničke pošte, IP i MAC adresa računala, GPS lokacija mobilnog uređaja, RFID tagovi, kolačići na web stranicama, fotografije, video snimke pojedinca, biometrijski podaci koje mogu prikupljati pametni telefoni (npr. otisak prsta, snimka šarenice oka), genetski podaci, podaci o obrazovanju i stručnoj spremi, podaci o plaći, kreditu, računu u banci, podaci o zdravlju, seksualnoj orijentaciji, glas i mnogi drugi koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. [5]

2.3. Uloge i odgovornosti

GDPR definira tri entiteta koja sudjeluju u procesu razmjene, čuvanja i obrade osobnih podataka, a koja donose i nove odgovornosti. To su:

- Subjekt obrade ili Ispitanik (eng. *Data Subject*)
- Voditelj obrade (eng. *Data Controller*)
- Izvršitelj obrade (eng. *Data Processor*)

Subjekt obrade, odnosno ispitanik, je svaka fizička osoba, građanin bilo koje od zemalja članica Europske Unije, čije podatke organizacija obrađuje. U kontekstu tvrtke, ispitanik može biti bilo koji korisnik, bivši korisnik, zaposlenik, kandidat za zaposlenje, ali čak i zaposlenik partnera. Ispitanik svoje osobne podatke dobrovoljno predaje Voditelju obrade.



Slika 2.1 Sudionici procesa [5]

Voditelj obrade je, sukladno članku 4. stavku 7. „fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima utvrđuje svrhe i sredstva obrade osobnih podataka“.[4]

Zakonska odgovornost voditelja obrade je velika, jer u trenutku kada ispitanik preda svoje osobne podatke voditelju obrade, on postaje vlasnikom tih podataka i brine da se podacima rukuje isključivo u svrhu za koju su predani. Tvrtka može biti voditelj obrade u situacijama kada samostalno kontrolira i odgovara za osobne podatke koje pohranjuje.

Izvršitelj obrade je, sukladno članku 4. stavku 8. GDPR-a, „fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade“.[4]

Primjer izvršitelja obrade može biti tvrtka koja za drugu tvrtku obrađuje podatke kandidata koji su prisustvovali natječaju za radno mjesto. U takvoj situaciji tvrtka u kojoj se kandidat prijavio za radno mjesto je voditelj obrade, a tvrtka koja obrađuje osobne podatke kandidata za zaposlenje je izvršitelj obrade.

Za potrebe marketinga jedna tvrtka može koristiti usluge druge tvrtke (npr. marketing putem elektroničke pošte, kampanje i slično). U tom je slučaju tvrtka koja nudi usluge marketinga putem elektroničke pošte izvršitelj obrade jer obrađuje osobne podatke potencijalnih kupaca.

Još jedna uloga, koja se pojavljuje stupanjem GDPR-a na snagu, je **Službenik za zaštitu podataka** (eng. *Data Processing Officer – DPO*).

Službenika za zaštitu podataka imenuje voditelj ili izvršitelj obrade, a njegova glavna zadaća je vođenje brige o zaštiti osobnih podataka. Osoba kojoj je dodijeljena ta uloga ne mora nužno biti zaposlenik tvrtke, već može biti i vanjski suradnik.

Službenik za zaštitu podataka treba biti upućen u pravo i prakse u području zaštite podataka, što uključuje dobro poznavanje sadržaja i primjene GDPR-a u poslovanju tvrtke. Ta osoba također treba poznavati politiku i interne akte tvrtke, poslovne procese i vrste obrade osobnih podataka, te pratiti poštivanje pravila o zaštiti osobnih podataka. Još neke od zadaća službenika za zaštitu podataka su podizanje svijesti i osposobljavanje sudionika procesa obrade osobnih podataka, pružanje savjeta vezanih za zaštitu osobnih podataka, suradnja i kontaktiranje nadzornog tijela oko nejasnoća prilikom načina obrade osobnih podataka ili u situacijama kada se sumnja na kršenje pravila zaštite osobnih podataka.

2.4. Nadzorno tijelo

Prema članku 51. GDPR-a, „Svaka država članica osigurava da je jedno ili više neovisnih tijela javne vlasti odgovorno za praćenje primjene ove Uredbe kako bi se zaštitila temeljna prava i slobode pojedinaca u pogledu obrade i olakšao slobodan protok osobnih podataka unutar Unije („nadzorno tijelo“)“. [4]

Dalje, prema Uredbi, nadzorno tijelo mora djelovati potpuno neovisno, a država je ta koja treba osigurati da nadzorno tijelo ima sve potrebne ljudske, tehničke i financijske resurse, prostor i infrastrukturu, kako bi moglo obavljati svoje zadaće.

Zadaće nadzornog tijela su da prati i provodi primjenu GDPR-a, osvješćuje javnost o rizicima, pravima, pravilima i mjerama zaštite u vezi s obradom osobnih podataka. Nadzorno tijelo treba pružati informacije ispitanicima na njihove upite o vlastitim pravima, rješavati njihove pritužbe, provoditi istrage, te također surađivati s nadzornim tijelima drugih država članica.

Sukladno sadržaju članka 58. GDPR-a, nadzornim tijelima su dodijeljene tri vrste ovlasti, a to su istražna, korektivna i savjetodavna.

Nadzorna tijela ovlaštena su zatražiti informacije o provođenju zaštite osobnih podataka, od voditelja i izvršitelja obrade, te također zatražiti uvid u osobne podatke i sve informacije potrebne za obavljanje svojih zadaća. Između ostaloga, nadzorna tijela ovlaštena su i za izdavanje privremenih ili konačnih zabrana obrade, za izricanje novčanih kazni i naređivanje suspenzija protoka podataka primatelju u trećoj zemlji ili međunarodnoj organizaciji.

U Republici Hrvatskoj je, za nadzorno tijelo, uspostavljena Agencija za zaštitu osobnih podataka (skraćeno AZOP). AZOP je posrednik između tvrtki i fizičkih osoba, te je zadužen za rješavanje problema i savjetovanje svih sudionika procesa obrade osobnih podataka.

3. Funkcionalni zahtjevi

Stupanjem GDPR-a na snagu, ispitanici su dobili nova prava, a tvrtke koje obrađuju njihove podatke su dobile nove obaveze. I prava i obaveze utječu na funkcionalne zahtjeve koji moraju biti ispunjeni.

Ispitanici imaju prava pristupati svojim podacima, znati na koji način se njihovi podaci obrađuju i koriste, tražiti ispravak podataka, ograničiti količinu podataka koji se obrađuju, tražiti isporuku svojih podataka kako bi ih koristili negdje drugdje, tražiti brisanje podataka i slično.

Tvrtke, s druge strane, trebaju moći demonstrirati ispitanicima da su osobni podaci koje obrađuju sigurni i zaštićeni, da koriste odgovarajuće metode upravljanja i kontrole podataka, da se podaci koriste na transparentan, odgovarajući, korektan i dozvoljen način, da posjeduju i koriste mjere smanjenja grešaka i ispravljaju greške, te da mogu poduzeti odgovarajuće akcije u slučaju curenja podataka ili bilo kakve povrede podataka.

Važno je napomenuti da se GDPR odnosi na sve tvrtke koje posluju ili u svojem poslovanju obrađuju osobne podatke građana Europske Unije, bez obzira na to gdje se nalazi sjedište tvrtke.

U funkcionalne zahtjeve koji se nameću tvrtkama koje obrađuju osobne podatke građana Europske Unije pripadaju:

- Izvješćivanje o povredi osobnih podataka (eng. *Breach Notification*)
- Pravo na pristup (eng. *Right to Access*)
- Pravo na zaborav (eng. *Right to be Forgotten*)
- Pravo na prenosivost podataka (eng. *Right to Data Portability*)

Navedena prava ispitanika bit će detaljno opisana u sljedećim poglavljima.

3.1. Izvješćivanje o povredi osobnih podataka

Povreda osobnih podataka definirana je u GDPR-u, a definicija glasi: „povreda osobnih podataka znači 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“. [4]

Povreda osobnih podataka može uključivati povredu nad financijskim podacima, što uključuje podatke o kreditnim karticama ili bankovnim računima i transakcijama. Može biti provedena nad podacima o zdravlju, podacima koji mogu identificirati pojedinca ili se odnose na korporativne tajne ili intelektualno vlasništvo. Najčešće povrede osobnih podataka uključuju izložene i ranjive nestrukturirane podatke, poput datoteka, dokumenata i osjetljivih informacija.

U slučaju sumnje na kršenje sigurnosti osobnih podataka, tvrtka je dužna u roku od 24 sata sumnju prijaviti službeniku za zaštitu podataka. Ukoliko službenik za zaštitu podataka utvrdi da je prijavljeno kršenje sigurnosti opravdano, podnosi prijavu nadležnom nadzornom tijelu. Obaveza prijave sumnje na povredu, odnosno same povrede osobnih podataka je unutar 72 sata od nastanka iste.

Na web stranicama Agencije za zaštitu osobnih podataka objavljen je obrazac izvješća o povredi osobnih podataka kojeg voditelji i izvršitelji obrade mogu koristiti u svom svakodnevnom radu. Izvješće sadrži podatke o voditelju obrade, sjedištu voditelja obrade, službeniku za zaštitu podataka, a u izvješću je potrebno opisati prirodu povrede osobnih podataka (što uključuje procijenjeno vrijeme nastupa povrede, kategoriju i približan broj ispitanika na koje se povreda odnosi), navesti posljedice koje povreda sa sobom nosi, te mjere koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje problema povrede osobnih podataka. [6]

3.2. Pravo na pristup

Prema članku 15. GDPR-a, ispitanik ima pravo tražiti i od voditelja obrade dobiti informaciju obrađuju li se njegovi osobni podaci. Ukoliko se podaci obrađuju, ispitanik može zatražiti pristup tim podacima, te informacije o tome u koju svrhu i na koji način se obrađuju, kome se prosljeđuju i slično.

Ovo pravo bilo je propisano i u ranije važećoj Direktivi 95/46/EZ, odjeljku V., članku 12. no u GDPR-u je puno detaljnije obrađeno i raspisano.

Ovaj zahtjev na prvu zvuči prilično jednostavnim i ne čini se da predstavlja problem, dok ne počnemo razmišljati na način kako u jednoj velikoj tvrtki znati na kojim se sve mjestima u sustavima, koji nisu integrirani, zaista nalaze svi podaci ispitanika. U današnje vrijeme, kada je tehnologija toliko napredovala, moguće je prikupljati podatke na razne načine, vrlo je teško bez dobro ustrojenih poslovnih procesa i sustava, utvrditi gdje se pojedini podatak zaista nalazi i u koju svrhu se on zaista i obrađuje.

U kontekstu GDPR-a, treba obratiti pozornost na sve što se smatra osobnim podatkom, što znači da nije dovoljno samo razmišljati kako podatke ispitanika pohranjujemo samo u obliku potpisanog ugovora o radu, ili u nekom od poslovnih sustava jer korisnik koristi naše usluge, već da se oni vrlo vjerojatno nalaze u našim arhivama, u ladicama i na računalima zaposlenika iz drugih odjela tvrtke ili smo ispitanika jednostavno snimili nadzornom kamerom koju iz sigurnosnih razloga imamo postavljenu ispred ulaza u tvrtku. Sada kada su nabrojane samo neke od situacija u kojima se mogu nalaziti osobni podaci ispitanika, slika postaje jasnija, a ispunjavanje zahtjeva kompliciranije.

Kako bi tvrtka ispunila ovaj zahtjev, trebala bi biti u mogućnosti sve te podatke objediniti i u najkraćem mogućem vremenu ispitaniku dostaviti odgovor na traženi zahtjev, a da pritom nešto od podataka ne promakne.

3.3. Pravo na zaborav

Pravo na zaborav, ili prema članku 17. GDPR-a, pravo na brisanje, označava pravo ispitanika da od voditelja obrade zatraži brisanje osobnih podataka koji se na njega odnose. Kako bi se ovo pravo realiziralo moraju biti ispunjeni neki od sljedećih uvjeta:

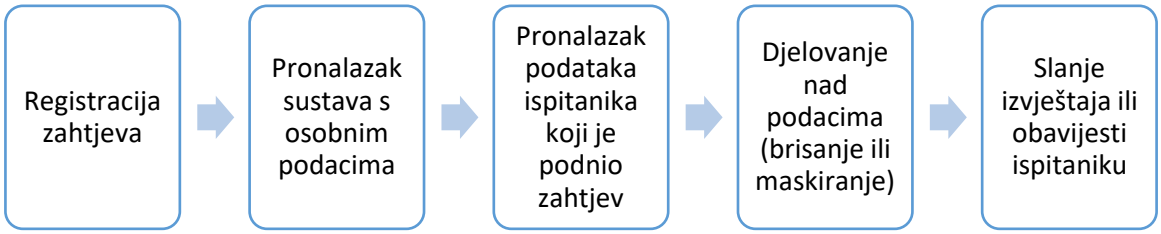
- Ne postoji svrha u koju bi se osobni podaci ispitanika dalje trebali obrađivati
- Ispitanik je povukao privolu na kojoj se temeljila obrada njegovih osobnih podataka
- Ne postoji druga pravna osnova za obradu
- Osobni podaci ispitanika su nezakonito obrađivani

Postoji nekoliko problema s kojima se tvrtke susreću prilikom ispunjavanja ovog prava. Prvi problem je identifikacija osobnih podataka ispitanika u svim IT sustavima jer se prilikom dizajna arhitekture ranijih IT sustava nije vodilo računa o ovakvim zahtjevima. Podatke je potrebno identificirati i ukloniti iz svih sigurnosnih kopija sustava, te arhiva podataka. Dodatne komplikacije nastaju ukoliko je tvrtka osobne podatke ispitanika proslijedila drugim tvrtkama na obradu, jer je tada potrebno i od tih tvrtki zatražiti uklanjanje osobnih podataka ispitanika.

Ono što je potrebno napomenuti jest da ovo pravo nije moguće ostvariti ukoliko postoji druga zakonska osnova sukladno kojoj je tvrtka dužna čuvati osobne podatke ispitanika. Primjerice, tvrtke su dužne čuvati podatke o isplatama plaća djelatnicima, pa nije moguće obrisati osobne podatke ispitanika iz sustava jer bi to imalo utjecaja na narušavanje integriteta samog sustava.

Možemo zaključiti da se ovo pravo najviše odnosi na situacije u kojima je ispitanik dao privolu za obradu vlastitih osobnih podataka, a manje na situacije u kojima je potpisan ugovor radi korištenja neke od usluga koju tvrtka, s kojom je ugovor sklopljen, nudi.

Primjer procesa prava na zaborav, iz prakse, sastoji se od sljedećih koraka:



Slika 3.1 Koraci procesa prava na zaborav, primjer iz prakse

3.4. Pravo na prenosivost podataka

Članak 20. GDPR-a glasi:

„Ispitanik ima pravo zaprimiti osobne podatke koji se odnose na njega, a koje je pružio voditelju obrade u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu te ima pravo prenijeti te podatke drugom voditelju obrade bez ometanja od strane voditelja obrade kojem su osobni podaci pruženi“. [4]

Kako bi se ovo pravo moglo ostvariti obrada se mora temeljiti na privoli i provoditi automatiziranim putem.

Ovo pravo je korisno u situaciji kada ispitanik npr. želi promijeniti trenutnog pružatelja usluge i s novim operaterom sklopiti ugovor o korištenju usluga, ponajviše jer štedi vrijeme. Podaci ispitanika trebali bi biti isporučeni u elektroničkom obliku novom operateru ili samom ispitaniku.

Važno je da su podaci u svakom slučaju kriptirani ili zaštićeni lozinkom, te da se ispitanik autentificira kako bi tvrtka koja isporučuje podatke bila sigurna da podatke zaista daje osobi na koju se odnose, a ne nekome drugome, što bi prouzročilo ogromne probleme.

4. Proces usklađivanja informacijskih sustava organizacije

Kako bi proces usklađivanja informacijskih sustava organizacije sa zahtjevima GDPR-a bio što jednostavniji i brži, svi sudionici tog procesa bi trebali biti svjesni trenutne usklađenosti s GDPR-om, odnosno količine posla koji je potrebno odraditi.

Prilikom pokretanja projekta usklađivanja tvrtke sa zahtjevima GDPR-a, jako je važno odabrati kvalitetan projektni tim. Projektni tim treba se sastojati od djelatnika iz svih ključnih segmenata poslovanja. U projekt bi, kao sponzori, prije svega trebala biti uključena Uprava tvrtke, odnosno najviši menadžment, čiji članovi bi trebali biti svjesni količine posla koju je potrebno odraditi. Uprava i menadžment bi trebali osigurati resurse koji će aktivno sudjelovati u procesu implementacije GDPR rješenja. Odgovor na pitanje zašto je baš Uprava toliko važna u samom projektu usklađivanja sa zahtjevima GDPR-a, jest iz razloga što su kazne propisane GDPR-om, u slučaju kršenja odredbi, jako visoke, odnosno iznose do 4% ukupnog godišnjeg prihoda ili 20 milijuna eura, u ovisnosti o tome što iznosi više.

Segmenti poslovanja koji se sigurno moraju uskladiti sa GDPR-om su:

- Pravna služba koja brine o internim aktima, te poslovnim ugovorima
- IT koji je centralno mjesto pohrane svih elektroničkih podataka
- Ljudski resursi koji pohranjuju ugovore i osobne podatke zaposlenika
- Marketing koji obrađuje podatke klijenata
- Financije koje pohranjuju podatke o plaćama zaposlenika
- Nabava koja surađuje s partnerima

Glavne faze procesa usklađivanja informacijskih sustava organizacije sa zahtjevima GDPR-a možemo podijeliti na sljedeće:

- Analiza stanja
- Analiza rizika
- Izrada plana sigurnosti podataka
- Integracija GDPR IT rješenja

U sljedećim poglavljima navedena su objašnjenja svake pojedine faze.

4.1. Analiza stanja

Prvi korak prilikom usklađivanja tvrtke s GDPR-om trebala bi svakako biti analiza stanja. Kako bi tvrtka znala otkuda krenuti s usklađivanjem, prvo bi trebala poznavati vlastite procese i sustave, odnosno znati gdje se sve unutar tvrtke pohranjuju podaci.

Analiza stanja trebala bi dati odgovore na pitanja poput:

- Kakve sve podatke pohranjujemo, kako ih koristimo i gdje se oni nalaze?
- Na kojim područjima poslovanja je potrebno napraviti promjene?
- Koji su to poslovni procesi na koje GDPR ima utjecaj?

Kako bi tvrtka napravila kvalitetnu analizu stanja potrebno je „prevesti“ zakonske, GDPR odredbe, u poslovne zahtjeve, koji su bliži ključnim korisnicima unutar tvrtke.

Ključna aktivnost prilikom usklađivanja informacijskih sustava organizacije sa zahtjevima GDPR-a je inventura i sređivanje (mapiranje) podataka koji se smatraju osobnima.

Inventurom podataka smatra se popisivanje svih osobnih podataka i povezanih informacija koje tvrtka ima o ispitaniku, a uključuje informacije o sljedećem:

- Vrsti podatka
- Kolekciji podatka
- Procesima u kojima podatak sudjeluje
- Prijenosima podatka
- Pohrani podatka
- Zaštiti podatka
- Zadržavanju podatka

Mapiranje podataka služi za identifikaciju osobnih podataka koji se prenose kroz različite poslovne sustave i načina na koje su ti podaci dijeljeni i organizirani. Mapiranjem identificiramo visokorizične obrade podataka koje dovode do procjena učinka na zaštitu podataka.

Inventura i mapiranje podataka rade se iz sljedećih razloga:

- Smanjenje mogućnosti rupa koje se pojavljuju između arhitekture na razini sustava i mapiranja procesnih tokova,
- Hvatanje ključnih informacija kako bismo bolje razumjeli detalje procesa obrade osobnih podataka,

- Procjena usklađenosti oko upotrebe, rukovanja i dijeljenja osobnih podataka

Kako bi inventura i mapiranje bili što efikasnije odrađeni, uz najmanji utrošak vremena, važno je podijeliti uloge. Ključni članovi svakog segmenta poslovanja u kojemu je potrebno usklađivanje s GDPR-om odrađuju svoj dio inventure. Potrebno je popisati sve poslovne procese koji se na segment poslovanja odnose, te pronaći sva mjesta (fizička i elektronička) na kojima se podaci pohranjuju. Rezultati se po mogućnosti pokušavaju minimizirati i strukturirati, što se odnosi ne samo na aktualne setove podataka, već i na povijesne.

Ključni korisnici u ovom dijelu procesa imaju važnu ulogu, jer su oni ti koji bi trebali znati koji su vremenski rokovi čuvanja određenih podataka, koji su načini pristupa i kome su zaista potrebna prava pristupa podacima. Za one podatke koji su se ranije čuvali bez definiranog roka, sada je potrebno definirati valjani rok čuvanja, koji će se ugraditi u tekstove privola i interne akte tvrtke. Također je potrebna analiza svih procesa obrade koji prema GDPR-u trebaju imati potpisanu privolu ispitanika, kako bi i ona postala dio redovitog procesa.

Inventura i mapiranje podataka mogu se odraditi na jedan od sljedeća tri načina:

- intervjuiranje ključnih korisnika i popunjavanje upitnika
- otkrivanje podataka korištenjem nekog od alata za automatsko skeniranje
- korištenjem API[1] integracije i povratnih informacija iz drugih sustava

Kao rezultat inventure podataka moguće je kreirati evidenciju aktivnosti obrade, o čemu je više riječi u sljedećem poglavlju.

4.1.1. Članak 30.: Evidencija aktivnosti obrade

Sukladno članku 30. stavcima 1. i 2. GDPR-a, svaki voditelj obrade i predstavnik voditelja obrade dužan je voditi evidenciju aktivnosti obrade za koje su odgovorni, te svaki izvršitelj obrade i predstavnik izvršitelja obrade dužan je voditi evidenciju svih kategorija aktivnosti obrade koje se obavljaju za voditelja obrade. Obveze iz stavaka 1. i 2. ne primjenjuju se na tvrtku ili organizaciju u kojoj je zaposleno manje od 250 osoba, osim:

[1] Sučelje programiranja aplikacije (eng. *Application programming interface*) – skup funkcija i postupaka koji omogućavaju stvaranje aplikacija koje pristupaju značajkama ili podacima operativnog sustava, drugih aplikacija ili servisa.

- ukoliko će obrada koju provodi vjerojatno prouzročiti visok rizik za prava i slobode ispitanika,
- ako obrada nije povremena ili obrada uključuje posebne kategorije podataka iz članka 9. stavka 1. ili
- ako je riječ o osobnim podacima u vezi s kaznenim osudama i kažnjivim djelima iz članka 10.

Evidencija aktivnosti obrade je osnovni preduvjet implementacije GDPR-a. GDPR ne zahtjeva detaljni inventar osobnih podataka, ali ga nije loše imati jer može biti koristan kao dio procesa upravljanja podacima.

Evidencija mora biti u pisanom obliku, uključujući elektronički oblik, te od strane voditelja obrade ili izvršitelja obrade, odnosno njihovih predstavnika, biti predana na uvid nadzornom tijelu, u slučaju kada nadzorno tijelo to zatraži. [4]

Ono što se promijenilo u odnosu na razdoblje prije stupanja GDPR-a na snagu, jest to što tvrtka više nije dužna redovito dostavljati evidenciju nadzornom tijelu, već ju je dužna dostaviti samo na njihov zahtjev.

Tvrtke mogu samostalno odlučiti koji će format evidencije aktivnosti obrade koristiti u poslovanju, jer on kao takav, nije definiran od strane GDPR-a. Savjet je da se evidencija pohranjuje na centraliziranom mjestu, po mogućnosti u zaštićenoj bazi podataka umjesto u običnoj Excel datoteci.

Ono što jest definirano su podaci koji se u evidenciji aktivnosti obrade moraju nalaziti. Osim kontakt podataka voditelja obrade, predstavnika obrade i službenika za zaštitu podataka, odnosno izvršitelja obrade i njegovog predstavnika u situacijama kada su to osobe izvan tvrtke, potrebno je navesti svrhu obrade svakog podatka, opise kategorija ispitanika i kategorije osobnih podataka koji se obrađuju. Također, potrebno je navesti i kategorije primatelja kojima se osobni podaci prosljeđuju na daljnju obradu ili uvid, te ukoliko je moguće, predviđene rokove za brisanje kategorija podataka i opis tehničkih i organizacijskih sigurnosnih mjera.

Sve navedeno ukazuje na to da je potrebno dobro poznavanje svih mjesta pohrane podataka unutar tvrtke, te poznavanje samih podataka kako bismo ih ispravno evidentirali. To je jedan od ključnih razloga zašto u projekt usklađivanja tvrtke sa zahtjevima GDPR-a trebaju biti uključeni ključni korisnici iz različitih segmenata poslovanja.

Primjera radi, djelatnik zaposlen u IT odjelu tvrtke vrlo vjerojatno poznaje osnovni proces odjela nabave, ali zasigurno ne zna u detalje koji su to osobni podaci koje nabava prikuplja, na koje ih načine obrađuje, u koje sve svrhe, te kako s njima postupa nakon završetka procesa. Isto vrijedi i za sve ostale segmente poslovanja.

Kvalitetan projektni tim će osim bržeg evidentiranja aktivnosti obrade i uštede vremena, biti i učinkovitiji.

Na slici 4.1 nalazi se primjer evidencije aktivnosti obrade osobnih podataka koje je Sveučilište u Zagrebu - Metalurški fakultet javno objavilo

SVEUČILIŠTE U ZAGREBU
METALURŠKI FAKULTET

UNIVERSITY OF ZAGREB
FACULTY OF METALLURGY

SISAK

EVIDENCIJA AKTIVNOSTI OBRADE OSOBNIH PODATAKA

POSLOVNI PROCES 2
STUDENT

1	2	3	4	5	6	7	8	9	10	11	12
ISPITANIK	OSOBNI PODATAK	IZVOR OSOBNOG PODATKA	SVRHA OBRADE	PRAVNI OSNOV OBRADE	NAČIN OBRADE	MJESTO OBRADE I POHRANE	ROK ČUVANJA	PRIMATELJ	ZAKONITOST OBRADE ČL. 6. GDPR	MJERE KONTROLE	PRAVA ISPITANIKA
student	podaci o studentu (ime, prezime, OIB, datum i mjesto rođenja, ime roditelja, adresa prebivališta, adresa boravišta, osobna fotografija)	student	studentski status, nastavni proces, ugovor o studiranju, obračun i isplata materijalnih prava na temelju ugovora ili odluka	Zakon o znanstvenoj djelatnosti i visokom obrazovanju	elektronički	Informacijski sustav visokih učilišta, sustav Merlin, nastavnici, Repozitorij, Aleph	trajno	Sveučilište u Zagrebu, Ministarstvo znanosti i obrazovanja, banka ustanove, banka studenta	članak 6. stavak 1. točka c	kontrola pristupa	pristup, ispravak
student	bankovni podaci (banka, IBAN, naziv banke)	student	obračun i isplata materijalnih prava na temelju ugovora ili odluka	Zakon o znanstvenoj djelatnosti i visokom obrazovanju	elektronički	Interno	trajno	Sveučilište u Zagrebu, Ministarstvo znanosti i obrazovanja	članak 6. stavak 1. točka c	kontrola pristupa	pristup, ispravak
student	podaci o elektroničkom identitetu	student, sistem inženjer	elektronička komunikacija	pravila o otvaranju i korištenju AAI, Sigurnosna politika CARNet	elektronički	sustav Merlin, nastavnici	trajno	Sveučilište u Zagrebu	članak 6. stavak 1. točka c	kontrola pristupa	pristup, ispravak
student	JMBAG	Informacijski sustav visokog obrazovanja	studentski status, nastavni proces	Zakon o znanstvenoj djelatnosti i visokom obrazovanju	elektronički	Informacijski sustav visokog obrazovanja	trajno	javno	članak 6. stavak 1. točka c	kontrola pristupa	pristup, ispravak
student	broj telefona, privatni elektronički identitet	student	elektronička komunikacija, komunikacija s vanjskim dionicima		elektronički	interno	trajno	vanjski dionici	članak 6. stavak 1. točka a	kontrola pristupa	pristup, ispravak

Slika 4.1 Evidencija aktivnosti obrade osobnih podataka sa Sveučilišta u Zagrebu, Metalurškog fakulteta

Kada se uspostavi evidencija aktivnosti obrade, sljedeći korak u usklađivanju je određivanje svrhe zbog koje se podaci ispitanika prikupljaju i obrađuju.

4.1.2. Članak 6.: Svrha obrade osobnih podataka

Kada govorimo o svrhama obrade osobnih podataka, one su od posebne važnosti za ovu temu. Članak 6. GDPR-a, pod nazivom „Zakonitost obrade“ govori upravo o svrhama obrade osobnih podataka, te propisuje sljedeće:

„Obrada je zakonita samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećega:

- Ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha
- Obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora
- Obrada je nužna radi poštovanja pravnih obveza voditelja obrade
- Obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe
- Obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade
- Obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete“ [4]

Osobni podaci mogu se čuvati za jednu ili više svrha koje su specifične, zakonite i jasno navedene, a podaci se trebaju obrađivati samo na način koji je sukladan sa konkretnom svrhom.

Kako bi se tvrtka prilagodila ovom zahtjevu GDPR-a, jedno od mogućih rješenja bi bilo implementirati sustav koji će na jednom mjestu imati evidenciju svih svrha obrade podataka, te poveznicu na same podatke koji se obrađuju. U slučaju da ne postoji zakonska svrha, a ispitanik nije dao privolu za obradu podataka, s jednog bi se mjesta moglo evidentirati koji su to podaci koje je potrebno ukloniti ili maskirati kako ne bi došlo do povrede osobnih podataka (u ovom slučaju iz razloga neopravdane obrade).

4.2. Analiza rizika

Tek kada je odrađena kompletna analiza stanja poslovnih procesa i informacijskih sustava, te je definirano na kojim se sve mjestima unutar tvrtke pohranjuju i obrađuju osobni podaci ispitanika, možemo govoriti o analizi rizika.

Cilj analize rizika je pokušati predvidjeti i spriječiti situacije u kojima bi se mogla dogoditi povreda osobnih podataka, te izraditi plan sigurnosti i implementirati sustave zaštite od povreda.

Prema članku 35., stavku 1. GDPR-a, definirana je procjena učinka na zaštitu podataka:

„Ako je vjerojatno da će neka vrsta obrade, osobito putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade prije obrade provodi procjenu učinka predviđenih postupaka obrade na zaštitu osobnih podataka. Jedna procjena može se odnositi na niz sličnih postupaka obrade koji predstavljaju slične visoke rizike.“

Proces koji je osmišljen kako bi tvrtkama pomogao da sustavno analiziraju, identificiraju i umanje rizike zaštite podataka (eng. *Data Protection Impact Assessment* ili skraćeno DPIA) nije specificiran od strane GDPR-a, ali je dio ključnih obaveza i odgovornosti u okviru GDPR-a. Ispravno urađen proces analize učinka zaštite podataka tvrtkama pomaže procijeniti i pokazati kako se pridržavaju svih obaveza zaštite podataka. Nije potrebno iskorijeniti sve rizike, ali bi provođenje ovog procesa tvrtkama trebalo pomoći umanjiti rizike i utvrditi je li razina rizika prihvatljiva u danim okolnostima, uzimajući u obzir prednost onoga što se želi postići.

Primjer predloška [7] za analizu procjene učinka na zaštitu podataka objavljen je na stranicama ICO-a (*Information Commissioner's Office*) u obliku kodeksa ponašanja za zaštitu podataka.

U njemu su navedena pitanja zaštite podataka, te je za svako pitanje definiran kodeks ponašanja, procjena rizika, dane su mjere ublažavanja i zaključak.

GDPR Analiza rizika			
GDPR Zahtjev	**Što to znači?**	**Gdje smo kao organizacija?**	**Što trebamo odraditi?**
1 - Svijest	Osigurati da su donositelji odluka i ključni ljudi u organizaciji svjesni stupanja GDPR-a na snagu. Provođenje GDPR-a moglo bi imati značajan utjecaj na uključenost resursa. Trebali bismo podići razinu svijesti o promjenama koje nas čekaju stupanjem GDPR-a na snagu.	Pokrenut je postupak podizanja svijesti i angažmana koji će biti potreban da bi se organizacija uskladila sa zahtjevima GDPR-a. Određeni datumi prvih sastanaka Uprave i direktora odjela radi odabira ključnih korisnika koji će sudjelovati u procesu usklađivanja tvrtke sa GDPR-om.	Proučiti Uredbu o zaštiti osobnih podataka i zahtjeve koje donosi. Kreirati prezentaciju kojom ćemo Upravi i direktorima prenijeti najvažnije informacije o zahtjevima GDPR-a. Odlučiti koji su okvirni rokovi i resursi potrebni u projektu usklađivanja organizacije s GDPR-om.
2 - Informacije koje posjedujemo	Dokumentirati osobne podatke koje posjedujemo, kako ih prikupljamo, na koji način ih obrađujemo i kome ih prosljeđujemo.	Izrađen je predložak Evidencije aktivnosti obrade, u obliku Excel tablice, u kojemu ćemo zabilježiti sve osobne podatke koje prikupljamo, na kojim mjestima, tko im ima pristup, koji su rokovi čuvanja tih podataka. Popisane su sve trenutne procedure i interni akti koje je potrebno pregledati i izmijeniti kako bismo bili usklađeni s GDPR-om. Izrađen je popis svih poslovnih sustava, web stranica i aplikacija koje tvrtka koristi.	Svaki odjel treba popuniti predložak Evidencije aktivnosti obrade kako bismo na jednom mjestu imali popis svih osobnih podataka koji se prikupljaju, pohranjuju i obrađuju unutar tvrtke. Pregledati postojeće procedure i procese, razmotriti situacije u kojima dolazi do višestrukih prikupljanja istih osobnih podataka pojedinaca, te ih doraditi na način da se minimiziraju osobni podaci. Uskladiti interne akte i ugovore sukladno GDPR-u. Povezati se s nadzornim tijelom radi informiranja o usklađivanju s GDPR-om.
3 - Komuniciranje podataka o privatnosti	Moramo pregledati naše trenutne obavijesti o privatnosti i staviti na raspolaganje plan za donošenje potrebnih izmjena.	Imamo obavijesti o prikupljanju osobnih podataka na web stranicama, ali nemamo jasno navedene svrhe za koje ih prikupljamo.	Osigurati da su naše obavijesti u skladu sa zahtjevima koje propisuje GDPR.
4 - Prava pojedinaca	Trebali bismo provjeriti naše procese, kako bismo osigurali da pokrivaju sva prava koja pojedinci imaju, uključujući i način brisanja osobnih podataka ili davanje podataka elektroničkim putem i u uobičajenom formatu. GDPR uključuje značajna poboljšanja: - pravo na pristup - ispravak netočnih podataka - brisanje podataka - sprječavanje izravnog marketinga - sprječavanje automatskog profiliranja i odlučivanja - prijenos podataka	U većini naših sustava su implementirane funkcionalnosti koje omogućavaju pokrivanje zahtjeva GDPR-a. Ne koristimo se izravnim marketingom.	U radu s direktorima trebamo utvrditi jesu li automatizirane prijave i profiliranje primjenjivi na tvrtku i osigurati da smo usklađeni s GDPR-om. Istražiti detaljnije zahtjeve za prijenosom podataka. Implementirati testnu verziju sustava za upravljanje privolama, kako bismo testirali sve funkcionalnosti i utvrdili mogućnosti izvršavanja zahtjeva koje nalaže GDPR. Pregledati podatke koji su dostupni korisnicima kako bismo bili sigurni da u potpunosti pokrivaju zahtjeve za pristup podacima.
5 - Zahtjev za pristup	Trebali bismo ažurirati procedure i planirati kako ćemo obrađivati zahtjeve u novim vremenskim okvirima: - Ne želimo plaćati kazne radi nepoštivanja zahtjeva - Trebamo utvrditi točne vremenske rokove za rješavanje zahtjeva	Trenutno postoji procedura kojom se definira proces odgovaranja tvrtke na zahtjeve ispitanika.	Pregledati politike i procedure vezane uz zahtjeve za pristup informacijama. Osigurati da su svi zaposlenici svjesni promjena koje su vezane uz zahtjev za pristup podacima prema GDPR-u.

6 - Pravna osnova za obradu osobnih podataka	Trebali bismo istražiti različite oblike obrade podataka koje provodimo, utvrditi našu pravnu osnovu za njihovo provođenje i dokumentiranje. Prema GDPR-u korisnici imaju pravo na brisanje podataka gdje nema opravdane svrhe za njihovo obrađivanje i pohranu. Morat ćemo objasniti pravnu osnovu za obradu podataka u obavijesti o privatnosti i prilikom odgovaranja na zahtjeve za pristup podacima.	Trenutno za obradu koristimo pravnu osnovu i privole korisnika (newsletter).	Osigurati da se preispitaju pravne osnove koje koristimo za obradu podataka, kako bismo bili sigurni da su u skladu s GDPR-om. Postaviti zakonske osnove za obradu u naše obavijesti o privatnosti. Osigurati osvješćivanje zaposlenika oko zahtjeva koje propisuje GDPR, vezano za obradu osobnih podataka.
7 - Privola	Trebali bismo pregledati na koje načine tražimo, dobivamo i bilježimo privole i trebamo li napraviti izmjene. GDPR jasno navodi da moramo moći dokazati da je privola dana od strane korisnika. Nadzorno tijelo upućuje da se, kad god je to moguće, trebamo osloniti na pravnu osnovu, umjesto traženja privole.	Trenutno pregledavamo pravne osnove za obradu osobnih podataka i pripremamo procjenu učinka na privatnost.	Pregledati i osnažiti obavijesti o privatnosti vezano uz pravnu osnovu za obradu. Pregledati politike i procedure. Pregledati metode prikupljanja privola.
8 - Djeca	GDPR donosi posebnu zaštitu osobnih podataka o djeci, posebice u kontekstu komercijalnih internetskih usluga kao što je društveno umrežavanje.	Ne obrađujemo podatke o djeci.	Provjeriti za svaki slučaj postoje li negdje u sustavima podaci o djeci koji se obrađuju.
9 - Povreda podataka	Trebali bismo osigurati da imamo odgovarajuće postupke za otkrivanje, prijavljivanje i istraživanje kršenja osobnih podataka. Morat ćemo izvijestiti o značajnim incidentima kršenja podataka nadzornom tijelu (AZOP) u roku od 72 sata nakon što postanemo svjesni povreda. GDPR prepoznaje da će u tom vremenskom razdoblju često biti nemoguće potpuno istražiti kršenje i omogućit će obavještavanje u fazama. Ukoliko je kršenje vjerojatno rezultiralo visokim rizikom za prava i slobode pojedinaca, morat ćemo obavijestiti oštećene vlasnike podataka. Novčane kazne mogu iznositi do 4% godišnjeg prihoda ili do 20 000 000 eura u ovisnosti što iznosi više. Ispitanici mogu prijaviti AZOP-u provjeru tvrtke ukoliko smatraju da su izloženi riziku od povrede podataka.	Postoji raspisana procedura koja se bavi povredama nad podacima.	Pregledati postojeće procese i procedure i utvrditi jesu li u potpunosti usklađene s GDPR-om. Dodatno educirati zaposlenike o načinu rukovanja s osobnim podacima klijenata koje obrađuju. Osigurati, koliko je moguće, da zaposlenici uklone sve nepotrebne kopije osobnih podataka sa svojih računala i mobilnih uređaja, te da djeluju maksimalno odgovorno prilikom izvršavanja obrada nad podacima.

10 - Dizajn zaštite podataka i Procjena učinka na zaštitu podataka	Trebamo procijeniti situacije u kojima će biti potrebno provesti procjenu utjecaja na zaštitu podataka. Svaki novi informacijski sustav mora sadržavati privatnost i zaštitu podataka u okviru svoje specifikacije. To će zahtijevati mogućnost revizije, povjerljiva područja, pristup temeljen na ulogama i kontrolu. Svaka nova usluga i sustav zahtijevaju DPIA sličan trenutnoj procjeni učinka privatnosti. Privatnost prema dizajnu i minimalizacija podataka uvijek su bili implicitni zahtjevi zaštite podataka. Međutim, GDPR je to učinio i zakonskim zahtjevima.	Svi poslovni sustavi koje tvrtka koristi imaju minimalno ugrađenu kontrolu pristupa podacima putem odgovarajućih korisničkih rola.	Provesti podizanje svijesti o zahtjevu za provođenje Procjene učinka na zaštitu podataka, kako bi se odrazile promjene GDPR-a. Poduzimati Procjenu učinka na novijim sustavima i odrediti rizik starijih sustava koje koristimo.
11 - Službenik za zaštitu podataka	GDPR zahtijeva da odredimo službenika za zaštitu podataka koji ima stručno iskustvo i znanje o zakonima zaštite podataka, a očekuje se da: - obavještava i savjetuje tvrtku i njene zaposlenike o njihovim obvezama u skladu s GDPR-om i drugim zakonima o zaštiti podataka - prati usklađenost s GDPR-om i drugim zakonima o zaštiti podataka, uključujući upravljanje unutarnjim aktivnostima zaštite podataka, savjetovanje o procjeni utjecaja na zaštitu podataka - bude prva točka kontakta nadzornom tijelu i ispitanicima čiji se podaci obrađuju Službeniku za zaštitu podataka treba dati adekvatne resurse koji će mu omogućiti ispunjavanje svojih obaveza. Službenik za zaštitu podataka mora izvještavati najvišu razinu menadžmenta, djelovati neovisno i imati odgovarajuće resurse.	Funkcija službenika za zaštitu podataka je već uvedena unutar tvrtke. Redovito izvještavanje prema najvišem menadžmentu tvrtke odvija se već u sklopu mjesečnih koordinacija ili po potrebi.	Provjeriti ima li službenik za zaštitu podataka sve potrebne resurse za obavljanje te funkcije. Omogućiti mu adekvatnu edukaciju i rasteretiti ga nekih drugih zadataka koji mogu utjecati na kvalitetu izvršavanja funkcije službenika za zaštitu podataka. Dogovoriti provođenje podizanja razine svijesti među zaposlenicima o ulozi službenika za zaštitu podataka i objasniti zaposlenicima koje su to ovlasti i odgovornosti službenika za zaštitu podataka.
12 - Međunarodni prijenos podataka	Ukoliko poslujemo međunarodno, trebamo provjeriti pod koje nadzorno tijelo pripadamo u tim situacijama.	Budući smo tvrtka registrirana u Hrvatskoj, nadzorno tijelo kojemu odgovaramo je Agencija za zaštitu podataka - AZOP.	Pregledati stranice AZOP-a i informirati se o ovlastima i propisima AZOP-a kao nadzornog tijela sukladno GDPR-u.

Kao dio ove osnovne analize, razmotreni su sljedeći dodatni elementi:			
13 - Odgovornost i upravljanje	Promjena u kulturi o odgovornostima i vlasništvu. Potrebno je osigurati da su svi zaposlenici svjesni svojih obaveza upravljanja i obrade podataka u skladu sa zakonskim zahtjevima. GDPR stavlja veći fokus na odgovornost, s voditeljima obrade podataka, koji su potrebni za dokazivanje sukladnosti. GDPR također uvodi nove dužnosti za izvršitelje obrade. Uvođenjem GDPR-a mogu se poduzeti mjere protiv izvršitelja obrade umjesto voditelja obrade podataka, ukoliko djeluju izvan uputa voditelja obrade.	U posljednjih 12 mjeseci poduzeti su koraci za jačanje podizanja svijesti o promjenama koje nastupaju stupanjem GDPR-a na snagu. To uključuje: promjene u internim aktima i procesima tvrtke, promjene ugovora potpisanih s vanjskim izvršiteljima obrade, podizanje svijesti, educiranje svih zaposlenika o GDPR-u, praćenje usklađenosti, imenovanje službenika za zaštitu podataka, implementacija sustava za upravljanje privolama, objava obavijesti na web stranicama.	Provjeriti sadržavaju li svi novi ugovori odgovarajuće klauzule koje se odnose na GDPR. Provoditi edukaciju svih novih zaposlenika o GDPR-u, te pravima i obvezama koje im se nameću, a kako bismo se zaštitili od povreda nad podacima. Redovno izvještavati najviši menadžment o statusu usklađenosti s GDPR-om.

Slika 4.2 Analiza rizika odrađena za potrebe projekta usklađivanja s GDPR-om, kreirana prema stvarnoj situaciji iz prakse

Rezultati analize rizika uvelike su olakšali izradu plana sigurnosti podataka.

4.3. Izrada plana sigurnosti podataka

Izrada plana sigurnosti podataka je sljedeća faza u kojoj se definiraju nedostaci između trenutnog i traženog stanja, identificiraju najbolja rješenja i rješavaju pitanja poput:

- Što je sve napravljeno?
- Koje su to organizacijske, a koje tehnološke promjene koje moramo implementirati?

Temeljem rezultata analize rizika tvrtka utvrđuje koje je tehničke mjere potrebno implementirati kako bi se zaštitila od povreda osobnih podataka.

Tehničkim mjerama se ponekad smatra samo zaštita osobnih podataka koji se nalaze na računalima i mreži, odnosno u informacijskim sustavima, što nije u potpunosti ispravno. Iako su računala i mreže od očigledne važnosti, mnogi sigurnosni incidenti mogu biti posljedica krađe ili gubitka opreme, nepravilnog otpisivanja starih računala i informacijske opreme, te gubitka tiskanih materijala ili njihovog neispravnog odlaganja. Tehničke mjere uključuju i fizičku i računalnu, odnosno informatičku sigurnost.

U tehničke mjere sigurnosti se ubrajaju:

- Zaštita prostorija alarmom i sigurnosna rasvjeta
- Kontrola pristupa prostorijama tvrtke i nadzor posjetitelja
- Raspolaganje tiskanim dokumentima i elektroničkim otpadom
- Održavanje informatičke opreme, osobito prijenosnih uređaja
- Sigurnost mreže i informacijskih sustava
- Sigurnost podataka koji su pohranjeni u sustavima, te osiguravanje kontrole pristupa
- Sigurnost web stranica i online aplikacija koje tvrtka koristi

S obzirom da se u ovom diplomskom radu opisuju načini usklađivanja informacijskih sustava tvrtke, na sljedećoj slici je naveden primjer plana sigurnosti proveden u praksi u sklopu projekta usklađivanja tvrtke s GDPR-om.

Plan sigurnosti podataka			
Oznaka	**Grupa aktivnosti**	**Aktivnost**	**Opis**
1.0.	Inventura i mapiranje podataka		
1.1.		Izrada tablice za evidenciju aktivnosti obrade	Izbor podataka koji će se evidentirati
1.2.		Održavanje radnog sastanka s odjelima	Podjela zadataka vezanih za popunjavanje evidencije aktivnosti obrade
1.3.		Popunjavanje evidencije aktivnosti obrade - svi odjeli zajedno	Popuniti Excel tablicu za evidenciju aktivnosti obrade, zapisati sva otvorena pitanja
1.3.1.		Evidencija marketinških podataka	Popisati sve marketinške podatke koje posjedujemo
1.3.2.		Evidencija matičnih podataka - Financije i Ljudski potencijali	Vidjeti na kojim se to mjestima preklapaju odjel Financija i Ljudskih potencijala kako bismo minimizirali količinu osobnih podataka koji se prikupljaju
1.4.		Popisivanje svih web stranica koje tvrtka koristi	Izraditi popis svih web stranica koje tvrtka koristi i podataka koji se na njima prikupljaju
1.5.		Inventura podataka o kontaktima	Kreirati jedinstveni popis svih kontakata, obrisati nepotpune i redundantne, one koji su potpuni pripremiti za učitavanje u Sustav za upravljanje privolama
1.6.		Revizija evidencije aktivnosti obrade	Revidirati popunjenu evidenciju aktivnosti obrade i temeljem iste odrediti koje su zadaće i aktivnosti koje tvrtka još mora odraditi kako bi bila u skladu s GDPR-om (privole, interni akti, izmjena procedura, ugovorne klauzule)
1.7.		Objava obavijesti o privatnosti na web stranicama	Odrediti tekstove za obavijesti o privatnosti i postaviti ih na sva web mjesta koja tvrtka koristi
1.8.		Izrada privola	Za svaku svrhu obrade koja nije zakonski uvjetovana, kreirati zasebnu privolu
1.8.1.		Slanje privola	Slanje privola ispitanicima u nekoliko faza, u svrhu kompletiranja maksimalnog mogućeg broja kontakata
1.9.		Inventura podataka u Konzaltingu	Edukacija zaposlenika o svrsi i potrebi provedbe inventure; Izrada popisa aktivnih projekata sa osobnim podacima
1.10.		Evidencija ugovora s voditeljima i izvršiteljima obrada	Definirati koje ugovore je potrebno izmijeniti ugradnjom dodatnih klauzula i radi potreba definiranja statusa izvršitelja obrade
1.11.		Uklanjanje podataka koji nemaju osnovu za čuvanje na sustavima tvrtke	Počistiti sve podatke koje nemamo potrebu čuvati i obrađivati, pogotovo pripaziti na kopije podataka koje su pohranjene na računalima zaposlenika, ukloniti podatke za koje nemamo privolu i svrhu za obradu
1.11.1.		Kreirati izjave da su svi podaci uklonjeni	Kreirati i dati zaposlenicima na ovjeru izjave kojima potvrđuju da su uklonili sve osobne podatke koji nemaju osnovu za čuvanje na sustavima tvrtke

2.0.	Revizija postojećih informacijskih sustava		
2.1.		Revizija kontrola pristupa u postojećim informacijskim sustavima	Revidirati postojeće informacijske sustave koji se koriste, napraviti reviziju rola i prava pristupa zaposlenika
3.0.	Implementacija sustava za upravljanje privolama		
3.1.		Izrada testnog okruženja	Instalacija rješenja na odabranom okruženju (MD Azure ili On premise); Definiranje testnog tima i uloga
3.2.		Učitavanje podataka sa podacima iz evidencije aktivnosti obrade	Unos evidencije obrada i raspoređivanje po odgovarajućim strukturama u sustavu za upravljanje privolama; konfiguracija uloga i prava korisnika aplikacije
3.3.		Povezivanje s drugim sustavima	Kreirati reference na druge sustave u aplikaciji
3.4.		Testiranje funkcionalnosti	Testiraju korisnici sukladno svojim privilegijama. Izlaz ove aktivnosti je lista eventualnih nedostataka i grešaka.
3.5.		Učitavanje svih potrebnih podataka i početak korištenja sustava za upravljanje privolama	Izrada kategorija podataka, vrsta podataka, kategorija ispitanika, podataka o izvršiteljima i voditeljima obrade, te primateljima podataka, i povezivanje na vanjske sustave
3.5.1.			Dodavanje procesnih aktivnosti, povezivanje sa vanjskim sustavima, izvršiteljima obrade, primateljima podataka, sigurnosnim mjerama
3.5.2.			Dodavanje svrha obrade i povezivanje sa procesnim aktivnostima
3.5.3.			Dodavanje privola i povezivanje privola sa svrhama obrade
3.5.4.			Kreiranje izvještaja za ispitanike, provjera funkcionalnosti zahtjeva na koje ispitanici imaju prava
3.5.5.			Izrada mapiranja podataka između izvornih sustava i sustava za upravljanje privolama, učitavanje pseudonimiziranih podataka iz izvornih sustava (vanjski identifikatori)
3.5.6.			Konfiguracija API-a i registracija vanjskih sustava sa pravima i rolama
4.0.	Edukacija i osvješćivanje zaposlenika		
4.1.		Osvješćivanje djelatnika o GDPR i značaju poštivanja odredbi	Edukacija zaposlenika o zahtjevima i propisima GDPR-a, načinu rukovanja s osobnim podacima klijenata, načinu upravljanja osobnim podacima općenito

Slika 4.3 Primjer plana sigurnosti provedenog u sklopu projekta usklađivanja tvrtke s GDPR-om

4.4. Integracija GDPR IT rješenja

Integracija GDPR rješenja, odnosno posljednja i najduža faza, čije trajanje ovisi o trajanju prethodnih faza, rezultira usklađivanjem organizacijske strukture, uvođenjem novih uloga i odgovornosti, dizajnom procedura i implementacijom sigurnosnih kontrola i sustavnih rješenja za koje se tvrtka odlučila.

Kada je tvrtka svjesna svojih rizika i izradila je plan sigurnosti osobnih podataka, te odabrala rješenja koja će koristiti u svrhu usklađivanja s GDPR-om, može započeti s integracijom GDPR rješenja.

Tipovi rješenja za koja se tvrtka može odlučiti su raznovrsni, a tu zasigurno pripadaju rješenja za otkrivanje i analizu polustrukturiranih ili nestrukturiranih podataka (eng. *Data discovery*), rješenja za maskiranje podataka i provođenje anonimizacije, enkripciju i slično.

Na tržištu u ovom trenutku postoje brojna razvijena rješenja za upravljanje privolama i usklađivanje tvrtke sa GDPR-om, a na samim tvrtkama je odluka koje rješenje će koristiti.

Detaljnije informacije o postojećim rješenjima i njihovoj primjeni nalaze se u sljedećim poglavljima.

5. Otkrivanje osobnih podataka

Kako bi tvrtka učinkovito upravljala osobnim podacima i bila ih u mogućnosti zaštititi, trebala bi se fokusirati na četiri ključna koraka :

- Otkrivanje podataka – identifikacija osobnih podataka koje tvrtka posjeduje i mjesta na kojima su ti podaci pohranjeni
- Upravljanje podacima – kako se pristupa podacima i kako ih se koristi
- Zaštita podataka – uspostavljanje sigurnosnih kontrola kako bi se spriječile ili otkrile povrede osobnih podataka
- Izvještavanje o podacima – bilo da se radi o odgovoru na zahtjev ispitanika, o prijavi povrede osobnih podataka nadzornom tijelu ili jednostavnom vođenju evidencije o obradi podataka

Osobni podaci u organizaciji se uobičajeno nalaze u sljedećim oblicima:

- Strukturirani elektronički podaci – baze podataka, aplikacije
- Polustrukturirani ili nestrukturirani elektronički podaci – dokumenti, poruke elektroničke pošte
- Ne-elektronički podaci – papirnate arhive, poslovni ugovori, tiskani izvještaji

U sljedećim poglavljima navedena su pojašnjenja svih oblika pohrane podataka unutar tvrtke.

5.1. Strukturirani elektronički podaci

Strukturirani elektronički podaci su svi podaci koji su organizirani u formatu kojeg na jednostavan način mogu koristiti baze podataka ili druge tehnologije. Uglavnom se odnose na informacije s visokim stupnjem organizacije, pohranjene u relacijskim bazama podataka koje je moguće pretraživati unosom jednostavnih upita ili korištenjem algoritama tražilice.[8]

Većina podataka unutar tvrtke je pohranjena u strukturiranom obliku, što se ponajviše odnosi na sustave za upravljanje odnosima s klijentima (CRM – *Customer Relationship Management System*). „Cilj CRM-a je organiziranje i automatizacija prodaje, marketinga i

službe pomoći te upravljanje svim informacijama u svezi klijenata na jednom mjestu i u jednom sustavu.“ [9]

Članak 4. GDPR-a, pod stavkom 6. navodi definiciju sustava pohrane, koja glasi: „sustav pohrane znači svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi“.

S obzirom da se u ovakvim sustavima krije velika količina osobnih podataka klijenata, potrebno ih je dobro zaštititi od neovlaštenog pristupa i curenja podataka.

Tehnike koje se koriste za otkrivanje strukturiranih osobnih podataka mogu biti:

- Profiliranje primarnog ključa – uključuje otkrivanje postotka jedinstvenih vrijednosti, te otkrivanje primarnih ključeva i kompozitnih primarnih ključeva
- Profiliranje entiteta – uključuje otkrivanje odnosa između grupa tablica i evaluaciju referencijalnih ključeva
- Profiliranje podatkovnih domena – uključuje otkrivanje grupa kolona na temelju uzoraka u imenu kolona, te otkrivanje grupa kolona na temelju uzorka u podacima

5.2. Nestrukturirani elektronički podaci

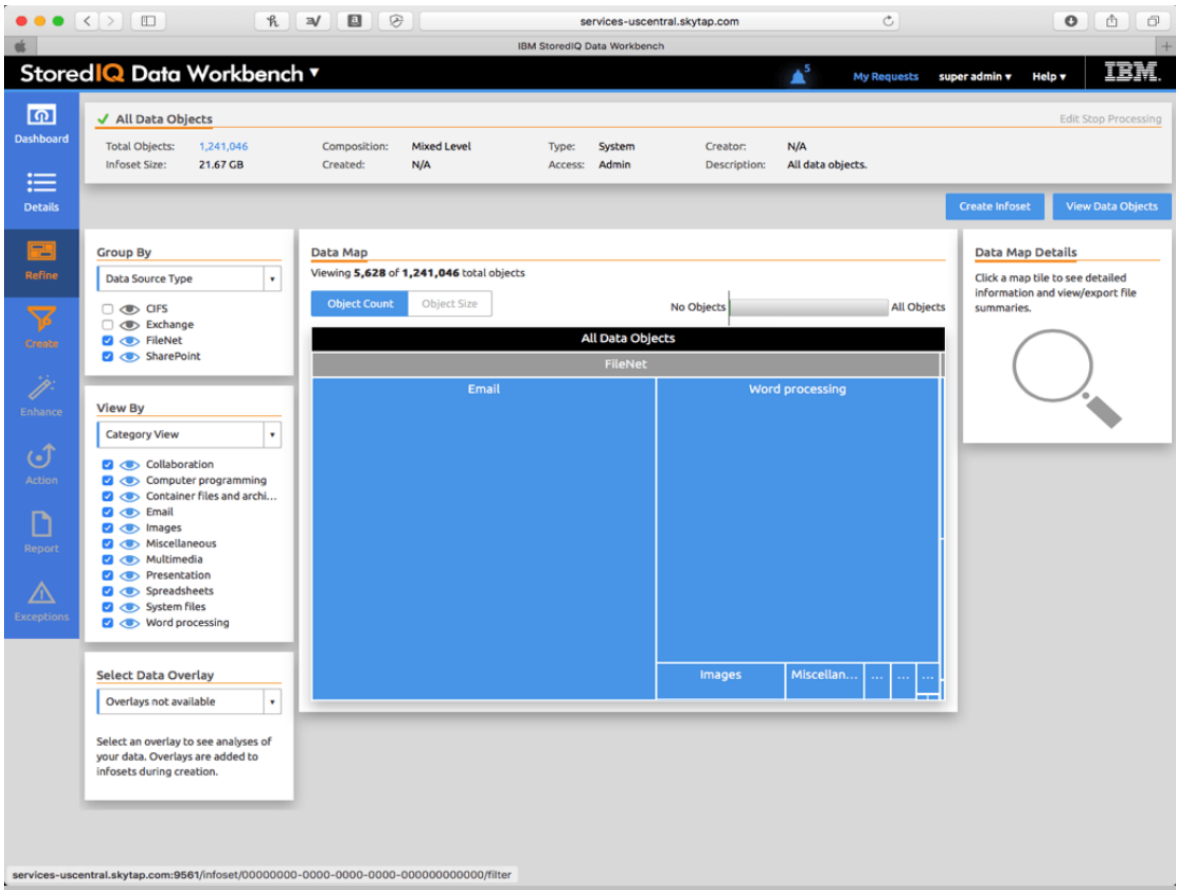
Nestrukturiranim podacima smatraju se svi ostali elektronički podaci koji imaju internu strukturu, ali nisu strukturirani korištenjem predefiniranih modela podataka. Tipični nestrukturirani podaci generirani od strane ljudi (a ne računala) su:

- Adresa elektroničke pošte – samo polje sadržaja poruke elektroničke pošte je nestrukturirano i tradicionalni analitički alati ga ne mogu sintaksno analizirati (parsirati)
- Društvene mreže – podaci s Facebook-a, Twitter-a, LinkedIn-a
- Web stranice – YouTube, Instagram, stranice za razmjenu slika
- Mobilni podaci – tekstualne poruke, lokacije
- Medijske datoteke – MP3, digitalne fotografije, zvučni i video zapisi
- Poslovne aplikacije – MS Office dokumenti, produkcijske aplikacije [8]

Zaposlenici svakodnevno koriste pametne telefone, elektroničku poštu, uredske elektroničke dokumente, radi izvršavanja poslovnih zadataka. Često se količina uredskih elektroničkih

dokumenata pohranjuje na više različitih mjesta, u nekoliko verzija, distribuira na *USB* prijenosnim uređajima, šalje porukama elektroničke pošte i slično. Ukoliko takvi dokumenti sadrže osobne podatke postaju predmetom GDPR-a. U kontekstu GDPR-a nestrukturirani podaci su puno kompliciraniji za zaštitu, te primjena tradicionalnih strukturiranih propisa nad njima nije jednostavna.

Brzi napredak tehnologije u posljednjih nekoliko godina doveo je do generiranja izuzetno velikih količina podataka. Na tržištu postoje alati za otkrivanje nestrukturiranih elektroničkih podataka, poput StoredIQ [10] tvrtke IBM. Jedan takav alat tvrtki omogućava otkrivanje, prepoznavanje i upravljanje nestrukturiranim podacima bez potrebe da se ti podaci prebacuju u zaseban repozitorij ili u druge aplikacije. Alati poput StoredIQ imaju ugrađene moćne tražilice koje tvrtkama ubrzavaju razumijevanje velikih količina nestrukturiranog sadržaja. Ono što je još važno je pojednostavljena analiza velikih količina korporativnih podataka, te mogućnost korištenja djelotvorne inteligencije koja podržava mnoge različite radnje u vezi s politikama i pravilima unutar tvrtke, a što uključuje kopiranje, brisanje, premještanje i izvoz nestrukturiranih podataka. IBM-ov StoredIQ sadrži kartu podataka (eng. *Data Map*) koja pruža izgled pohranjenih podataka i dubinske informacije o vrstama izvora podataka, kategorijama podataka, veličini ili količinama, broju podatkovnih objekata i njihovim pojedinostima.



Slika 5.1 Prikaz izgleda ekrana IBM StoredIQ alata za pretraživanje nestrukturiranih elektroničkih podataka

5.3. Ne-elektronički podaci

U ne-elektroničke podatke spadaju svi papirnati dokumenti, kopije dokumenata, ugovori, kopirane osobne iskaznice i ostale vrste dokumenata, ali i sve ispisane poruke elektroničke pošte, razni izvještaji iz poslovnih sustava i njihove kopije, koje se najčešće vrlo jednostavno i nekontrolirano dijele među zaposlenicima, nezaštićeno ostavljaju na stolovima nakon radnog vremena, spremaju po ladicama i registratorima, a sadrže mnoštvo osobnih podataka.

Ovu kategoriju podataka je najteže zaštititi jer je nemoguće pregledati i ukloniti sve papire i provjeriti njihov sadržaj. Tvrtka se ipak može zaštititi od generiranja ovakvih podataka provođenjem edukacije zaposlenika i učestalog osvješćivanja o važnosti zahtjeva GDPR-a, propisivanjem procedure uništavanja papira, propisivanjem internih akata o smanjenju generiranja pisanih kopija dokumenata, digitalizacijom procesa papirnatih dokumenata i uvođenjem ugovora o tajnosti.

6. Upravljanje i zaštita osobnih podataka

6.1. Kontrola pristupa podacima

Kada govorimo o kontroli pristupa podacima, često zaboravljamo koliko je važna, ne samo softverska, već i fizička kontrola pristupa podacima.

Kontrolu pristupa podacima možemo ostvariti na više načina. Neki od njih su korištenje enkripcije, autentikacije korisnika, korištenje rola za pristup podacima i slično.

U svim poslovnim sustavima je potrebno uvesti kontrole pristupa podacima. Poslužitelji bi primjerice trebali biti zaključani u zasebnoj prostoriji u koju je ograničen, ili preporučeno, zabranjen pristup djelatnicima koji nisu zaposlenici odjela IT-a. Današnje poslovne aplikacije imaju funkcionalnost kontrole pristupa implementiranu do mjere da je moguće samostalno kreirati grupe korisnika i dodavati im ovlaštenja za pristup samo određenim segmentima i podacima aplikacije.

Ono što tvrtka treba napraviti po pitanju kontrole pristupa podacima jest dobro definirati što koji djelatnik radi, kojim podacima zaista treba imati pristup i sukladno tome mu dodijeliti ovlaštenja za rad u sustavu. Ne smije se dogoditi da svi imaju prava pristupa svemu jer to dovodi do velikih sigurnosnih rizika.

Česte su situacije da djelatnici mijenjaju posao, odlaze kod drugih poslodavaca, a prilikom odlaska sa sobom odnose čitave baze podataka pohranjene na prijenosnim uređajima za pohranu ili slično. Kako bi se tvrtka osigurala od takvih povreda nad podacima, potrebno je ograničiti pristup podacima.

Ukoliko tvrtka za svoje poslovanje koristi operativni sustav Microsoft Windows, jedan od osnovnih načina kontrole pristupa podacima je korištenjem imeničkog servisa *Microsoft Active Directory Domain Services* (skraćeno AD DS). *Active Directory* je baza podataka koja vodi evidenciju o svim „objektima“ u sustavu na način da s jednog centraliziranog mjesta definira i ažurira sva prava pojedinih objekata na mreži. Pod objektima se u ovom kontekstu misli na korisnike, računala, sigurnosne grupe, servise i slično. Objekti se svrstavaju u organizacijske jedinice nad kojima se primjenjuju grupna pravila. [11]

Jedna od temeljnih postavki trebala bi svakako biti ona koja zaključava korisničko računalo nakon samo nekoliko minuta neaktivnosti čime se sprječava pristup podacima na računalu u

slučaju kada korisnik nije aktivan. Česte su situacije u kojima korisnici prilikom rada moraju fizički odstupiti od računala, a ukoliko pritom ostavljaju računala nezaštićenima povećavaju rizik od neovlaštenog pristupa podacima od strane drugih korisnika ili posjetitelja.

Podatke ne bi trebalo kopirati po raznim prijenosnim uređajima jer na taj način gubimo kontrolu nad količinom generiranih podataka i povećavamo mogućnost povrede koju je kasnije teško otkriti. Dodatne preporuke su također i korištenje enkripcije nad podacima, bilo da se radi o enkripciji tvrdih diskova, ili enkripciji koju koristimo za slanje podataka putem *online* kanala. [12]

Otkako su na tržište došli pametni uređaji, sigurnost podataka se uvelike smanjila. Svaki djelatnik na svojem mobilnom uređaju zasigurno ima aplikaciju za korištenje elektroničkom poštom, kako bi mogao komunicirati neovisno o tome je li blizu računala ili nije. Tu su i velike količine fotografija, poslovnih dokumenata koji stižu kao privitci poruka elektroničke pošte, glasovnih zapisa i slično. Trebamo biti svjesni svih funkcionalnosti današnjih pametnih telefona, te pravovremeno educirati i stalno osvješćivati korisnike o mogućnostima zaštite ukoliko dođe do krađe ili gubljenja istih, a sve s ciljem djelotvornije zaštite u takvim situacijama. Neki od načina povećanja sigurnosti su korištenje pina za otključavanje ekrana, dvostruka provjera autentičnosti, te osiguranje u slučaju gubitka ili krađe uređaja, na način da je omogućeno brisanje podataka, s takvih uređaja, na daljinu.

6.2. Zaštita osobnih podataka na izvoru – anonimizacija podataka

GDPR preporuča anonimizaciju, pseudonimizaciju i minimizaciju podataka kao specifične načine zaštite osobnih podataka. Sve tri tehnike mogu se konkurentno koristiti nad istim podacima.

Anonimizacija podataka jedna je od ključnih tema GDPR-a, a označava korištenje jedne ili više tehnika dizajniranih u svrhu onemogućavanja identifikacije pojedinca iz seta podataka koji su o njemu pohranjeni. Kada govorimo o anonimizaciji podataka mislimo na uklanjanje informacija.

Tehnike korištene prilikom anonimizacije podataka mogu biti *blanking*, *hashing* ili maskiranje osobnih identifikatora.

Blanking označava tehniku kojom se podaci štite na način da ih se mijenja s prazninama, odnosno uklanja.

Hashing je tehnika kojom se podatak anonimizira na način da se umjesto podatka umeću znakovi poput *hash* „#“ znaka.

Maskiranje osobnih identifikatora je tehnika kojom se osobni identifikatori zamjenjuju naizgled realnim podacima istog tipa, kako bi se sakrile stvarne vrijednosti podataka, ali omogućilo nesmetano testiranje podataka.

Anonimizirani osobni podaci više se ne smatraju osobnim podacima i na taj način prestaju biti predmetom bavljenja GDPR-a. Na ovaj način tvrtke mogu koristiti podatke za puno šire svrhe, a da pri tome ne krše prava o zaštiti podataka.

Na sljedećem primjeru objašnjeno je kako točno funkcionira anonimizacija podataka, te kako izgledaju podaci prije i poslije korištenja tehnike anonimizacije.

Recimo da odjelu marketinga u nekoj tvrtki trebaju podaci o prodaji proizvoda kako bi mogli kreirati kvartalnu statističku analizu i vidjeti koji su to proizvodi koji se najviše, odnosno najmanje prodaju, te odlučiti u kojem smjeru voditi marketinšku kampanju. IT odjel bi trebao isporučiti podatke o prodaji proizvoda iz baze podataka narudžbi kupaca. Prije stupanja GDPR-a na snagu, odjel marketinga bi dobivao kompletan set podataka izvučenih iz baze o narudžbama kupaca, uključujući i osobne podatke kupaca, koji im za svrhu kreiranja analize prodaje proizvoda zaista nisu bili potrebni. Tablica 6.1 prikazuje podatke koje bi odjel marketinga mogao dobiti od IT odjela.

Proizvod	Šifra kupca	Adresa	Telefonski broj	Količina	Ukupan iznos	Datum
Proizvod A1	0001	Ulica Frana Alfirevića 4	091 123 4567	12	600,00	1.3.2018
Proizvod B2	0002	Ulica Stjepana Radića 22	092 234 5678	25	20.000,00	12.5.2018
Proizvod C3	0003	Ulica grada Vukovara 81	095 345 6789	57	5.700,00	26.6.2018
Proizvod D4	0004	Ulica Divka Budaka 15	097 456 7890	3	1.275,00	16.2.2018
Proizvod E5	0005	Ulica Ante Jakšića 9	098 567 8901	21	2.100,00	30.1.2018
Proizvod F6	0006	Ulica Javora 13	099 678 9012	8	4.000,00	3.5.2018
Proizvod G7	0007	Ulica Maćuhica 260	091 890 1234	40	2.800,00	14.4.2018

Tablica 6.1 Primjer podataka izvučenih iz baze narudžbi kupaca

Ono što je vidljivo na setu podataka iz primjera jest da se u setu nalaze podaci poput adrese i telefonskog broja kupca, koje je moguće povezati sa kupcem i na taj ga način identificirati.

Ono što GDPR propisuje je striktna zabrana pristupa osobnim podacima ispitanika i obrada tih podataka u svrhe koje nisu zakonski opravdane poslovne svrhe ili tvrtka za njih nije dobila privolu od ispitanika.

Odjel marketinga može napraviti analizu prodaje proizvoda i ukoliko nema pristup osobnim podacima kupaca, jer im oni za analizu niti nisu potrebni.

U tablici 6.2 prikazan je set podataka koji je marketingu potreban kako bi analizirao prodaju proizvoda.

Proizvod	Količina	Ukupan iznos	Datum
Proizvod A1	12	600,00	1.3.2018
Proizvod B2	25	20.000,00	12.5.2018
Proizvod C3	57	5.700,00	26.6.2018
Proizvod D4	3	1.275,00	16.2.2018
Proizvod E5	21	2.100,00	30.1.2018
Proizvod F6	8	4.000,00	3.5.2018
Proizvod G7	40	2.800,00	14.4.2018

Tablica 6.2 Podaci koji su dovoljni za analizu prodaje proizvoda

Primjenom tehnike anonimizacije podataka IT odjel može nepovratno anonimizirati osobne podatke iz seta podataka, te ih takve isporučiti odjelu marketinga. Na ovaj način osobni podaci su zaštićeni i nije ih moguće povezati sa stvarnim kupcima.

Tablica 6.3 prikazuje set podataka nad kojima je primijenjena anonimizacija.

Proizvod	Šifra kupca	Adresa	Telefonski broj	Količina	Ukupan iznos	Datum
Proizvod A1	0001	Ulica ######	09# ### ####	12	600,00	1.3.2018
Proizvod B2	0002	Ulica ######	09# ### ####	25	20.000,00	12.5.2018
Proizvod C3	0003	Ulica ######	09# ### ####	57	5.700,00	26.6.2018
Proizvod D4	0004	Ulica ######	09# ### ####	3	1.275,00	16.2.2018
Proizvod E5	0005	Ulica ######	09# ### ####	21	2.100,00	30.1.2018
Proizvod F6	0006	Ulica ######	09# ### ####	8	4.000,00	3.5.2018
Proizvod G7	0007	Ulica ######	09# ### ####	40	2.800,00	14.4.2018

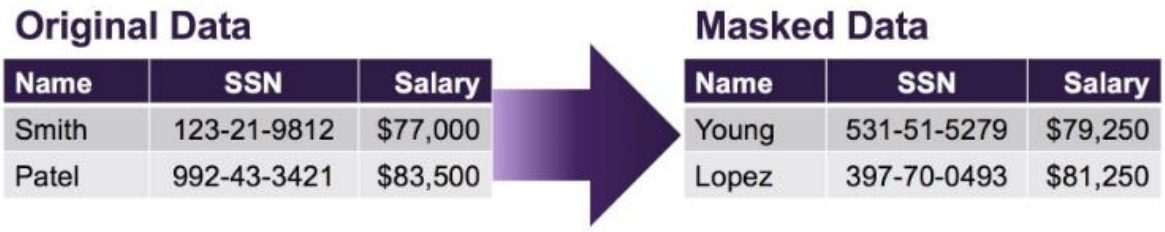
Tablica 6.3 Anonimizirani set podataka

Osobni podaci anonimizirani su na način da su stvarne adrese i brojevi telefona zamijenjeni znakom „#“, te ih više nije moguće povezati sa stvarnim kupcima.

6.3. Maskiranje podataka

Maskiranje podataka je proces zaštite povjerljivih informacija skrivanjem ili promjenom podataka, kako bi originalna vrijednost bila neprepoznatljiva, a služi za osiguravanje privatnosti podataka.

Korištenjem maskiranja podataka, podatke nije moguće ponovno identificirati, te podaci koji su maskirani prestaju biti predmetom GDPR-a.



Slika 6.1 Primjer maskiranih podataka

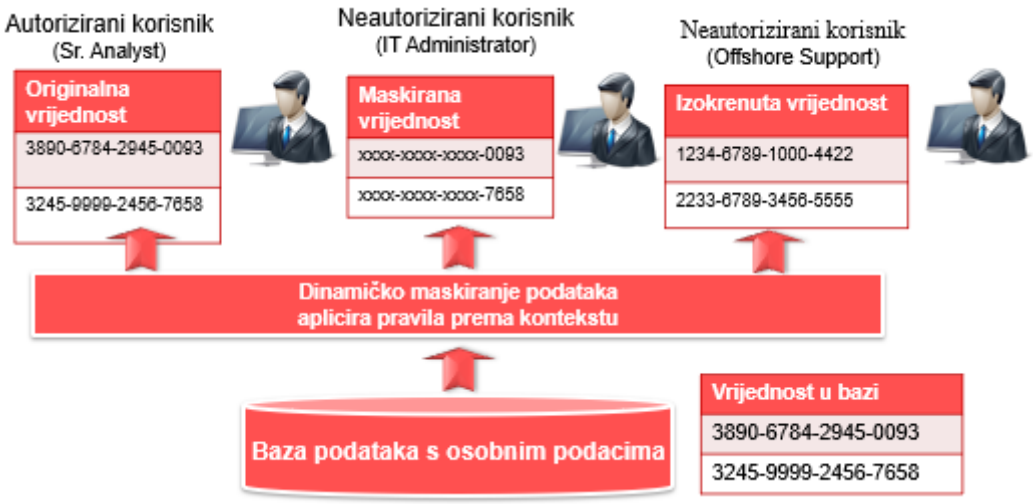
Tvrtke koje u svojem poslovanju koriste produkcijske podatke najčešće već imaju dobro zaštićena okruženja. Što se tiče razvojnih i testnih okruženja, ona su potencijalno rizična. Zaštita osobnih podataka koji se nalaze u takvim okruženjima nije samo moralna odgovornost tvrtke, već u određenim slučajevima zahtijeva i vladajući standard. Podaci koji se nalaze u takvim okruženjima mogu pripadati zaposlenicima klijenta ili same tvrtke, a curenje takvih podataka tvrtki može donijeti visoke kazne i velike probleme.

Postoji više vrsta maskiranja podataka, a u nastavku je objašnjena podjela na statično i dinamičko maskiranje.

Statično maskiranje (perzistentno) se koristi nad podacima u razvojnim i testnim okruženjima. Statičnim maskiranjem podatke u sustavu mijenjamo realističnima, ali ne i realnim podacima. Na taj način osigurava se zaštita podataka, ali i valjanost i mogućnost testiranja testnih podataka, što je svrha korištenja maskiranja. Mana kod korištenja ovakvog maskiranja je što se maskiranje provodi nad bazom podataka korištenjem *batch* procesa (ne u stvarnom vremenu), što može potrajati od nekoliko minuta, do nekoliko sati za dovršenje procesa, ovisno o veličini podataka. Statično maskiranje se nikako ne smije provoditi nad produkcijskim podacima jer trajno mijenja originalne podatke u bazi.

Kako bi se maskiranje provodilo nad produkcijskim podacima, koristimo se **dinamičkim maskiranjem**. Dinamičko maskiranje koristi se kada podacima pristupaju korisnici, bez da se maskiraju originalne vrijednosti podataka. Na taj način korisnicima se omogućava uvid u

samo one podatke za koje imaju prava pristupa. Tehnologija je smještena između aplikacija i baza podataka i uobičajeno se koristi za sustave koji spremaju velike količine osjetljivih podataka.



Slika 6.2 Prikaz rezultata dinamičkog maskiranja podataka

Dinamičko maskiranje funkcionira na način da prilikom slanja upita bazi podataka, *proxy* poslužitelj baze podataka mijenja upit, u ovisnosti o roli korisnika koji ga je uputio.

Recimo da korisnik, koji nema prava vidjeti podatke o broju kartice, pošalje sljedeći upit prema bazi:

```
select broj_kartice from korisnik_tbl
```

Baza provjerava koja prava ima korisnik koji je poslao upit, te u ovisnosti o roli korisnika, mijenja dobiveni upit u sljedeći:

```
SELECT concat('XXXX-XXXX-XXXX-', substring(broj_kartice,15,4))
                    from korisnik_tbl
```

Rezultat upita bi u tom slučaju izgledao ovako:

broj kartice (originalni)	broj kartice (maskirani)
1473-2251-8390-3099	XXXX-XXXX-XXXX-3099
2672-8773-2341-6454	XXXX-XXXX-XXXX-6454
9448-3620-3868-5114	XXXX-XXXX-XXXX-5114

Tablica 6.4 Primjer rezultata dohvaćanja podataka koji su dinamički maskirani

Za postavljanje pravila maskiranja potrebno je detaljno mapiranje aplikacija, korisnika, objekata baze podataka i prava pristupa. Održavanje takve matrice konfiguracijskih podataka zahtijeva značajan napor.

Kako bismo prilikom maskiranja podataka bili sigurni da ćemo prikazati realne ali ne i originalne podatke iz sustava, a da pritom ne izgubimo originalne podatke, ne smijemo maskirati jedinstvene identifikatore. Identifikatori bi mogli biti primarni ključevi u bazi podataka, te bismo primjenom enkripcije nad takvim podacima ili izmjenom tih podataka, mogli ugroziti integritet i veze među stvarnim podacima u bazi. Ukoliko ipak odlučimo maskirati identifikatore, tada sve instance identifikatora, svugdje u bazi, moramo maskirati u istu vrijednost.

Na tržištu danas postoje mnogobrojna rješenja za maskiranje podataka, poput *IBM Infosphere Optim Data Masking Solution, Oracle Data Masking Solution, Informatica Dynamic Data Masking, HP Test Data Management* i drugih.

7. Privola ispitanika

GDPR u Članku 4. navodi definiciju privole:

„Privola“ ispitanika znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose. [4]

Privole se primjenjuju na sve građane Europske Unije, zaposlenike, poslovne partnere, klijente i treće pravne osobe, a voditelji obrade moraju dobiti privolu ispitanika za obradu osobnih podataka u svim situacijama kada obrada podataka nije zakonski utemeljena.

Privole nisu novost, koristile su se i prije GDPR-a, samo ih GDPR detaljnije definira. GDPR zahtijeva da se privole kreiraju na način da ispitaniku jasno i jednoznačno navode svrhu za koju tvrtka namjerava obrađivati njegove podatke. Ukoliko tvrtka želi ispitanikove podatke obrađivati u više različitih svrha, sve moraju biti zasebno navedene i jasno definirane, a ispitanik za svaku mora dati privolu. Privole moraju biti afirmativno napisane, odnosno ispitanik se potpisivanjem privole treba izjasniti o tome da želi ustupiti svoje podatke na obradu tvrtki.

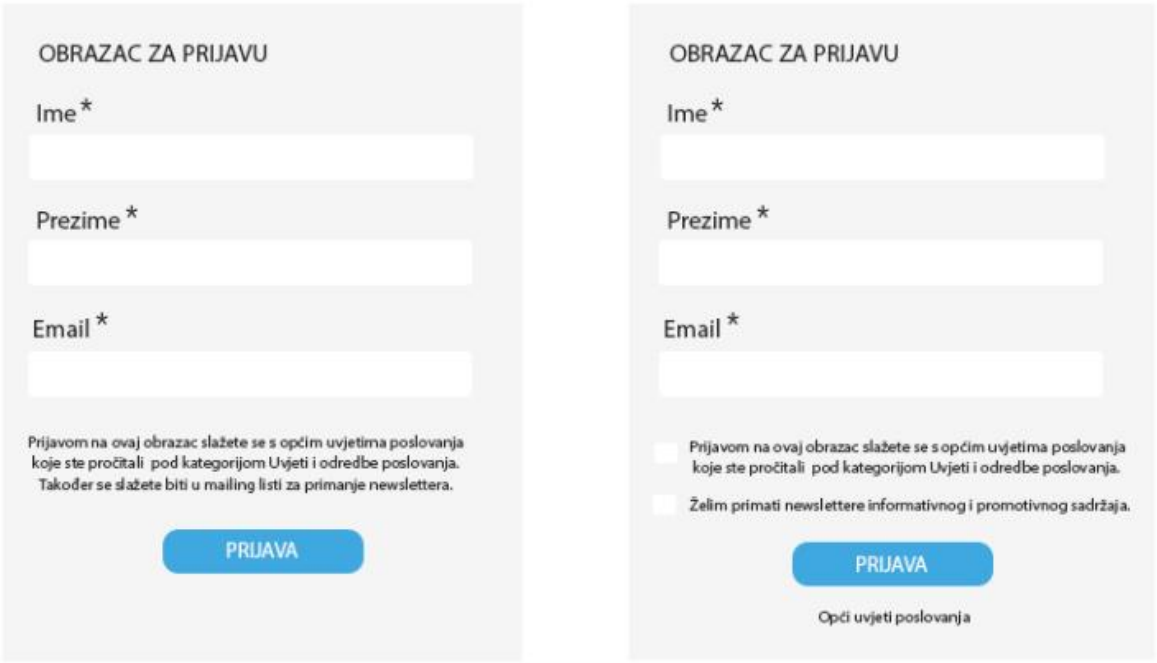
Ni u kojem slučaju nije dozvoljeno da svrha obrade bude unaprijed „označena kvačicom“ (online privole na web stranicama) ili da privolom ispitanik negira davanje suglasnosti za obradu podataka, kao niti da usluga bude uvjetovana davanjem privole ispitanika.

Dobra praksa je, u tekst privole, navesti i trajanje razdoblja korištenja i čuvanja podataka, a neki od savjeta su prikupljati osobne podatke pošteno i transparentno čime, ne samo da tvrtka ulijeva dodatno povjerenje kod ispitanika, nego i povećava ispitanikovu svijest o obradi podataka te smanjuje rizik od povreda učinjenih nad istima.

Još jedno od novih prava ispitanika je i mogućnost povlačenja privole. U situacijama kada ispitanik odluči da ne želi više davati privolu za obradu svojih osobnih podataka u svrhe navedene privolom, tvrtka mu mora omogućiti povlačenje privole, te prestati obrađivati njegove osobne podatke.

Postoje situacije u kojima je uvijek potrebno tražiti privolu ispitanika, a to su one kada tvrtka želi obrađivati posebne kategorije osobnih podataka. U te kategorije spadaju biometrijski i genetski podaci, rasno ili etničko podrijetlo, politička stajališta, sindikalno članstvo, zdravlje, spolni život i slično.

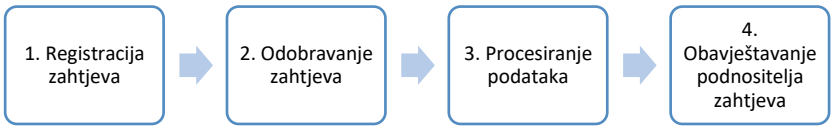
Na slici 7.1 je naveden primjer neispravne i ispravne privole kojom se od ispitanika zahtijevaju osobni podaci poput imena, prezimena i adrese elektroničke pošte.



Slika 7.1 Primjer neispravne i ispravne privole za prikupljanje osobnih podataka ispitanika [13]

8. Proces upravljanja zahtjevima ispitanika

Jedan od načina efikasnog upravljanja zahtjevima ispitanika jest implementacija sustava koji će službeniku za zaštitu podataka i voditeljima obrade omogućiti jednostavnije upravljanje ispitanicima, njihovim zahtjevima, privolama i svrhama. Takav sustav trebao bi ispitanicima omogućiti uvid u dane privole i svrhe za koje se njihovi osobni podaci obrađuju i koriste, ali i podnošenje zahtjeva na koje imaju pravo.



Slika 8.1 Koraci procesa upravljanja zahtjevima ispitanika

Koraci procesa upravljanja zahtjevima ispitanika trebali bi biti sljedeći:

- Podaci o zahtjevima se preuzimaju s korisničkog kanala
- Zahtjevi se evidentiraju kroz sustav za vođenje zahtjeva
- Automatska evaluacija za korak dokazivanja provjere autentičnosti
- Proces odobravanja zahtjeva unutar organizacije
- Identifikacija sustava za izvršavanje zahtjeva
- Propagacija zahtjeva na izvršavanje u identificirane sustave
- Izvršavanje na sustavima
- Prihvaćanje statusa i priprema odgovora za korisnički portal

Kako bi sustav upravljanja zahtjevima ispitanika, bio još efikasniji, unutar njega bi trebao biti ugrađen i sustav za upravljanje ispitanicima.

Jedan od načina je da unutar sustava postoje reference na sve postojeće sustave, što znači da bi tvrtka sa jednog mjesta mogla imati uvid u sve sustave koji pohranjuju i obrađuju osobne podatke ispitanika. Ova funkcionalnost rješava pitanje prava ispitanika za pristup podacima, ali i poštivanje načela o transparentnosti obrade osobnih podataka.

U situacijama kada ispitanika zanima obrađuju li se njegovi osobni podaci, za koje svrhe i koji su to osobni podaci, iz jednog ovakvog sustava mu se u relativno kratkom roku može odgovoriti na sva pitanja. Ideja nije da se podaci dupliciraju i pohranjuju u još jedan od sustava u kojemu će se vršiti obrada osobnih podataka, već da se u takvom sustavu

pohranjuje samo eksterni identifikator na osobni podatak u bazi u kojoj je isti i pohranjen. Centralizirano se pristupa svim referencama na pojedine sustave koji pohranjuju i obrađuju podatke ispitanika, a kao sustav zaštite se obavezno koristi anonimizacija i kontrola pristupa.

Sustav olakšava posao i službeniku za zaštitu osobnih podataka, ali i voditelju obrade. Na jednom mjestu postoji informacija o tome što je ispitanik zatražio, koje podatke o njemu posjedujemo, gdje su oni pohranjeni i za koje svrhe se obrađuju.

Kako je opisano u poglavlju 4.1.1., tvrtka sukladno GDPR-u ima obavezu voditi evidenciju aktivnosti obrade. Ranije je bilo potrebno evidenciju dostavljati Agenciji za zaštitu osobnih podataka, no od uvođenja GDPR-a to više nije obavezno.

U slučaju kada se sumnja na povredu osobnih podataka, ispitanik ili tvrtka koja obrađuje podatke ispitanika, mogu se obratiti AZOP-u, a vrlo je vjerojatno da će AZOP od tvrtke tražiti evidenciju aktivnosti obrade na uvid.

Evidencija aktivnosti obrade može također biti implementirana kao dio cjelovitog rješenja za upravljanje zahtjevima ispitanika ili se može voditi zasebno, ali ju je potrebno konstantno nadograđivati i ažurirati, što je zadatak službenika za zaštitu osobnih podataka, kao i voditelja obrade.

Ukoliko na jednome mjestu unutar tvrtke, a u ovom slučaju je to u sustavu za upravljanje zahtjevima ispitanika, imamo informaciju o tome koji podaci, kojeg ispitanika, za koje svrhe se obrađuju, vrlo je jednostavno ispuniti zahtjev za dostavom evidencije aktivnosti obrade nadzornom tijelu.

Kako je već ranije navedeno, u poglavlju 4.1.2., svrhama obrade se posvećuje poprilična pažnja kada je u pitanju GDPR. Svaka obrada podataka se mora temeljiti na nekoj svrsi. Ukoliko svrha nije zakonski regulirana, tvrtka koja obrađuje osobne podatke ispitanika, obradu smije temeljiti isključivo na potpisanoj privoli od strane ispitanika.

Tvrtka se prilikom usklađivanja s GDPR-om mora zaštititi od mogućnosti povrede osobnih podataka, a kako bi smanjila mogućnost povrede, voditelji obrade bi trebali imati informaciju smiju li obrađivati osobne podatke ispitanika.

Ispitanik ima pravo ispitati svrhu za koju tvrtka pohranjuje i obrađuje njegove podatke, a tvrtka treba biti u mogućnosti identificirati tu svrhu.

Sustav za upravljanje zahtjevima ispitanika koji bi mogao biti centralno mjesto pohrane svih privola, svih ispitanika, treba imati i mogućnost upravljanja svrhama, jer se privola potpisuje

kako bi se tvrtki dalo pravo da osobne podatke obrađuje za navedenu svrhu. U slučaju da ispitanik odluči povući danu privolu, voditelji obrade imali bi istovremeno informaciju o tome koje podatke više ne smiju obrađivati.

9. Primjer softverskog rješenja

Tvrtka, Poslovna inteligencija d.o.o., kreirala je vlastito softversko rješenje u obliku Sustava za upravljanje privolama, koje na jednom mjestu integrira i brine o mnogim zahtjevima GDPR-a, poput maskiranja podataka, enkripcije, fizičke zaštite dostupa itd.

Rješenje je razvijeno u obliku web aplikacije sa vlastitom bazom podataka, koja može biti SQL Server, Oracle ili DB2. Slanje informacija iz aplikacije se odvija putem API-ja prema ESB-u (eng. *Enterprise Service Bus*) ili izravno prema postojećim „*legacy*“ sustavima (zastarjeli sustavi koji se još uvijek koriste).

Aplikacija je zamišljena kao osnovno sredstvo rada budućih službenika za zaštitu podataka i voditelja obrada, ali isto tako i kao centralno mjesto na kojemu će ispitanici moći dobiti sve informacije o vlastitim podacima, načinima i svrhama obrade, privolama i ostalome što propisuje GDPR.

Sustav se sastoji od brojnih funkcionalnosti:

- Registar procesnih aktivnosti
- Upravljanje ispitanicima
- Upravljanje životnim tijekom privole
- Upravljanje zahtjevima ispitanika
- Upravljanje ugovorima
- Otkrivanje podataka – odnosi se na baze podataka i sustave sa strukturiranim podacima
- Korisnički portal
- Privole za kolačiće
- Sef sigurnosti podataka
- Upravljanje tokovima podataka

Korištenjem jednog ovakvog sustava automatiziran je cijeli proces, od registracije zahtjeva, preko procesa odobravanja zahtjeva i procesiranja podataka, do obavještavanja podnositelja zahtjeva o ishodu. Omogućena je potpuna kontrola nad svim procesima vezanim za upravljanje privolama ispitanika i njihovim zahtjevima.

Prilikom implementacije rješenja važno je obratiti pažnju na to stvara li se istovremeno još jedna baza osobnih podataka korisnika, o kojoj će netko morati brinuti, ili se putem rješenja

samo povezuje na centralnu bazu podataka bez spremanja stvarnih osobnih podataka ispitanika.

10. Zaključak

Od stupanja GDPR-a na snagu došlo je do promjena u načinu na koji postupamo s osobnim podacima. Najavljene kazne poprilično su utjecale na povećanje važnosti usklađivanja tvrtki s GDPR-om. Tvrtke su već imenovale ili će morati imenovati službenike za zaštitu podataka koji će brinuti o sukladnosti sa svim zahtjevima, informirati o povredama ispitanika te educirati zaposlenike kako bi se povrede podataka maksimalno umanjile, odnosno spriječile.

Velike tvrtke će se zasigurno naći u težoj situaciji jer se podaci u takvim tvrtkama pohranjuju u velikom broju različitih poslovnih sustava koji nisu međusobno integrirani. Situaciju dodatno kompliciraju nova prava ispitanika koja je uveo GDPR, a koja zahtijevaju funkcionalne promjene u informacijskim sustavima. Kako bi tvrtke mogle odgovoriti na zahtjeve, moraju poznavati vlastite sustave, odnosno osobne podatke koje prikupljaju. Nisu svi podaci strukturirani i lako pretraživi, već se u velikom broju nalaze u nestrukturiranim oblicima (porukama elektroničke pošte, uredskim elektroničkim dokumentima i slično). Na tržištu postoje razvijena rješenja koja omogućavaju pretragu nestrukturiranih podataka, ali takva rješenja iziskuju i velika ulaganja.

Zaštitu osobnih podataka moguće je olakšati uvođenjem kontrola pristupa, odnosno dodjelom korisničkih rola i privilegija nad određenim dijelovima sustava i bazama podataka. Podatke ne produkcijskih i testnih sustava je potrebno maskirati kako bi se razvoj i testiranja takvih sustava i dalje mogli provoditi, a kako ne bi bila moguća povreda osobnih podataka.

Prvi korak prilikom usklađivanja tvrtke sa zahtjevima GDPR-a svakako je izrada analize stanja tvrtke prilikom koje se otkrivaju sva mjesta pohrane podataka. Kao rezultat analize stanja moguće je kreirati evidenciju aktivnosti obrade. Kada je tvrtka svjesna svih mjesta na kojima se podaci nalaze može napraviti analizu rizika temeljem koje će se izraditi plan sigurnosti osobnih podataka. Ono što bi trebao biti rezultat analize rizika je odabir rješenja koja je potrebno implementirati te revizija poslovnih procesa i internih akata na način da budu usklađeni s GDPR-om. Posao koji očekuje tvrtke je velik i važno je da najviši menadžment, na čelu s Upravom, bude svjestan situacije u kojoj se tvrtka nalazi, kako bi se izbjegla plaćanja visokih kazni.

Uvođenje novih poslovnih rješenja u postojeći sustav može imati velike posljedice na kompletno poslovanje tvrtke, odnose unutar postojećih poslovnih cjelina i na odnose s

vanjskim izvršiteljima obrade. Stoga je važno prije svega definirati, sagledati sve poslovne rizike i tek tada krenuti u implementaciju rješenja za usklađivanje s GDPR-om.

Popis kratica

GDPR	*General Data Protection Regulation*	Opća uredba o zaštiti podataka
DPO	*Data Processing Officer*	Službenik za zaštitu osobnih podataka
CRM	*Customer Relationship Management*	Sustav za upravljanje klijentima
API	*Application Programming Interface*	Sučelje za programiranje aplikacija
DPIA	*Data Protection Impact Assessment*	Procjena učinka na zaštitu podataka
ESB	*Enterprise service bus*	Sabirnica usluga

Popis slika

Slika 2.1 Sudionici procesa [5] 6

Slika 3.1 Koraci procesa prava na zaborav, primjer iz prakse 12

Slika 4.1 Evidencija aktivnosti obrade osobnih podataka sa Sveučilišta u Zagrebu, Metalurškog fakulteta 19

Slika 4.2 Analiza rizika odrađena za potrebe projekta usklađivanja s GDPR-om, kreirana prema stvarnoj situaciji iz prakse 25

Slika 4.3 Primjer plana sigurnosti provedenog u sklopu projekta usklađivanja tvrtke s GDPR-om 28

Slika 5.1 Prikaz izgleda ekrana IBM StoredIQ alata za pretraživanje nestrukturiranih elektroničkih podataka 33

Slika 6.4 Primjer maskiranih podataka 38

Slika 6.5 Prikaz rezultata dinamičkog maskiranja podataka 39

Slika 7.1 Primjer neispravne i ispravne privole za prikupljanje osobnih podataka ispitanika 42

Slika 8.1 Koraci procesa upravljanja zahtjevima ispitanika 43

Popis tablica

Tablica 6.1 Primjer podataka izvučenih iz baze narudžbi kupaca 36

Tablica 6.2 Podaci koji su dovoljni za analizu prodaje proizvoda 37

Tablica 6.3 Anonimizirani set podataka 37

Tablica 6.4 Primjer rezultata dohvaćanja podataka koji su dinamički maskirani 40

Literatura

[1] *Prijedlog zakona 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*
http://www.sabor.hr/fgs.axd?id=4742 15.08.2018.

[2] EUROPEAN DATA PROTECTION SUPERVISOR – *The History of the General Data Protection Regulation*
https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en 15.08.2018.

[3] *DIREKTIVA 95/46/EZ EUROPSKOG PARLAMENTA I VIJEĆA od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka*
https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:31995L0046&from=en 15.08.2018.

[4] 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 (Opća uredba o zaštiti podataka)
https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&from=EN 15.08.2018.

[5] BIONDIC, N. *Što je to GDPR (General Data Protection Regulation)?*15.11.2017.
https://www.talentlyft.com/hr/blog/article/76/sto-je-to-gdpr-general-data-protection-regulation

[6] AGENCIJA ZA ZAŠTITU OSOBNIH PODATAKA *Izvješće o povredi osobnih podataka*
http://azop.hr/zbirke-osobnih-podataka/detaljnije/izvjesca-o-povredi-osobnih-podataka 15.08.2018.

[7] INFORMATION COMMISSIONER'S OFFICE *How do we carry out a DPIA?*
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-carry-out-a-dpia/
15.08.2018.

[8] TAYLOR, C. *Structured vs. Unstructured Data* 28.03.2018.
https://www.datamation.com/big-data/structured-vs-unstructured-data.html

[9] BIZIT *Što je CRM I što se iza njega krije* 24.01.2016.
https://www.bizit.hr/sto-je-crm-i-sto-se-iza-njega-krije/

[10] IBM *IBM StoredIQ Suite*
https://www.ibm.com/hr-en/marketplace/ibm-storediq-suite/details 15.08.2018.

[11] INTEGRA GROUP *Active Directory*
https://www.integragroup.hr/usluge-i-rjesenja/infrastruktura/active-directory
15.08.2018.

[12] GDPR INFORMER *Osnove zaštte podataka: Kontrole pristupa* 18.04.2018.
https://gdprinformer.com/hr/gdpr-clanci/osnove-zastite-podataka-kontrole-pristupa

[13] ARBONA – AGENCIJA ZA DIGITALNI MARKETING *GDPR i prikupljanje osobnih podataka: nekoliko "kvaka" koje će vam olakšati život* 15.05.2018. https://www.arbona.hr/blog/internet-ili-internetski-marketing/gdpr-i-prikupljanje-osobnih-podataka-nekoliko-kvaka-koje-ce-vam-olaksati-zivot/724

Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada.

U Zagrebu, _____

_____