PRIVREDNA BANKA ZAGREB

POLITIKA O ZAŠTITI OSOBNIH PODATAKA

srpanj 2018.

SADRŽAJ

1. UVOD

Dana 27. travnja 2016. godine Europski parlament i Vijeće usvojili se Uredbu 2016/679 o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka – Opća uredba o zaštiti podataka (nadalje: GDPR ili Uredba). Uredba se primjenjuje od 25. svibnja 2018. godine, čime se van snage stavlja prijašnja Direktiva 95/46/EC te se izravno primjenjuje u svim državama članicama.

Europsko zakonodavstvo nametnulo je svakom voditelju obrade odgovornost za provedbu odgovarajućih regulatornih, organizacijskih i tehnoloških mjera kako bi postiglo usklađenost s propisanim zahtjevima u skladu s pristupom temeljenim na procjeni rizika (tzv. načelo pouzdanosti).

Točnije, bilo kakva obrada osobnih podataka koju provode voditelj obrade ili izvršitelj obrade koji su osnovani ili djeluju unutar Europske unije moraju biti u skladu s ovim propisom, bez obzira provodi li se obrada unutar Europske unije ili izvan nje te provode li je voditelji obrade ili izvršitelji obrade koji nisu osnovani u Europskoj uniji te obrađuju li osobne podatke ispitanika koji su u Europskoj uniji.

Pravo na zaštitu osobnih podataka, odnosno pravo na privatnost, temeljno je ljudsko pravo vezano uz zaštitu ljudskoga dostojanstva, kako se to također utvrđuje u Povelji Europske unije o temeljnim pravima.

Iako joj je formalni cilj zaštita osobnih podataka fizičkih osoba, Uredba uvodi načela i standarde zaštite koji se primjenjuju, kao najbolja praksa, na sve podatke koje obrađuje voditelj obrade, uključujući i obradu podataka pravnih osoba, budući da takvi podaci mogu također imati eventualne značajne utjecaje na naknadu štete i ugled.

Ova Politika definira načela odgovornosti, zadataka i makro-procesa u upravljanju rizikom neusklađenosti u pogledu zaštite osobnih podataka za Banku i članice Grupe osnovane u Europskoj uniji.

2. PRIMJENJIVI REGULATORNI OKVIR

Kao što je naznačeno, glavna regulatorna referenca o zaštiti osobnih podataka sastoji se od Opće uredbe o zaštiti podataka (EU) 2016/679 (engl. General Data Protection Regulation, ili GDPR) kojom se zahtijeva sljedeće:

- primjena načela tehničke zaštite podataka i integrirane zaštite podataka kako bi se zajamčilo praćenje rizika nepoštovanja zakonodavstva o zaštiti privatnosti, u fazama stvaranja ili značajne promjene u obradi osobnih podataka te tijekom obrade, usvajanjem prethodno utvrđenih prikladnih tehničkih i organizacijskih mjera u svrhu osiguranja odgovarajuće razine sigurnosti
- izrada i kontinuirano ažuriranje Evidencije aktivnosti obrade
- provođenje Procjene utjecaja na privatnost (PIA) prije nastavka jedne ili više obrada koje mogu predstavljati visok rizik za prava i slobode ispitanika fizičkih osoba
- imenovanje Službenika za zaštitu podataka
- imenovanje osoba ovlaštenih za obradu
- imenovanje izvršitelja obrada, kad je to potrebno
- utvrđivanje mogućih zajedničkih voditelja obrade i formaliziranje vezanih ugovora

- izrada i održavanje popisa kontrola koji se odnose na privatnost
- obavijest o povredi osobnih podataka AZOP-u i komunikaciji s ispitanicima
- primjena mjera za osiguranje učinkovite provedbe prava ispitanika koja su definirana Uredbom
- organiziranje edukacijskih aktivnosti i širenje kulture privatnosti

u svrhu primjene GDPR-a, Radna skupina iz članka 29. istaknula je također sljedeće smjernice koje uključuju nacionalna nadzorna tijela u svrhu zaštite osobnih podatka europskih zemalja:

- Smjernice o automatiziranom pojedinačnom odlučivanju i izradi profila u svrhu Uredbe 2016/679 (wp251);
- Smjernice o obavijesti o povredi osobnih podataka u skladu s Uredbom 2016/679 (wp250);
- Smjernice o privoli u skladu s Uredbom 2016/679 (wp259);
- Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade "vjerojatno prouzročiti visok rizik" (wp248);
- Smjernice o službenicima za zaštitu podataka (wp243);
- Smjernice o transparentnosti u skladu s Uredbom 2016/679 (wp260);
- Smjernice o pravu na prenosivost podataka (wp242);
- Mišljenje 2/2017 o obradi podataka na radnom mjestu
- Mišljenje 6/2014 o pojmu legitimnih interesa voditelja obrade u skladu s člankom 7. Direktive 95/46/EC.

Svaka povreda odredbi GDPR-a podliježe upravnim novčanim kaznama u iznosu do 4% ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, neovisno o pravu na naknadu štete koju je pretrpio ispitanik.

3. DEFINICIJE

Za potrebe ovog dokumenta utvrđuju se sljedeći pojmovi:

"Deidentifikacija" obrada osobnih podataka na taj način da se više ne omogućava identifikacija ispitanika

"Nadzorno tijelo" neovisno tijelo javne vlasti koje je osnovala država članica u skladu s člankom 51. GDPR-a (Agencija za zaštitu osobnih podataka u Hrvatskoj).

"Predmetno nadzorno tijelo" nadzorno tijelo koje je povezano s obradom osobnih podataka zato što: a) voditelj obrade ili izvršitelj obrade imaju poslovni nastan na području države članice tog nadzornog tijela; b) obrada bitno utječe ili je izgledno da će bitno utjecati na ispitanike koji borave u državi članici tog nadzornog tijela; c) podnesena je pritužba tom nadzornom tijelu.

"Privola ispitanika" svaka dobrovoljna, posebna, informirana i nedvosmislena naznaka volje ispitanika pristanak ispitanika kojom on, izjavom ili jasnom potvrdnom radnjom, izražava suglasnost za obradu osobnih podataka koji se odnose na njega.

"Zajednički voditelji obrade" dva ili više voditelja obrade koji zajednički odrede svrhe i načine obrade

"Povreda podataka" kršenje sigurnosti koje dovodi do povrede povjerljivosti, dostupnosti ili integriteta osobnih podataka te obuhvaća rizik za prava i slobode fizičkih osoba. Povreda osobnih podataka može se prijaviti nadzornom tijelu te, na posljetku, ispitanicima.

"Službenik za zaštitu podataka" uspostavljen u skladu s GDPR-om.

"Osobni podaci" svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, uključujući trgovce pojedince i slobodna zanimanja („ispitanik"), pri čemu je pojedinac čiji se identitet može utvrditi 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, genetički, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.

"Biometrijski podaci" 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.

Genetski podaci – osobni podaci koji se odnose na naslijeđena ili stečena genetička obilježja pojedinca koja daju jedinstvenu informaciju o fiziologiji ili zdravlju tog pojedinca i koji su dobiveni osobito analizom biološkog uzorka dotičnog pojedinca.

Podaci koje se odnose na zdravlje – osobni podaci povezani s fizičkim ili mentalnim zdravljem pojedinca, uključujući pružanje zdravstvenih usluga, kojima se daju informacije o njegovu zdravstvenom statusu.

Primatelj – fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana. Međutim, tijela javne vlasti koja mogu primiti osobne podatke u okviru određene istrage u skladu s pravom EU-a ili države članice ne smatraju se primateljima; obrada tih podataka koju obavljaju ta tijela javne vlasti mora biti u skladu s primjenjivim pravilima o zaštiti podataka prema svrhama obrade.

"Hrvatska Agencija za zaštitu osobnih podataka" – nadzorno tijelo nadležno za nadzor provođenja propisa o zaštiti privatnosti u Hrvatskoj

"Pravo na ograničavanje obrade" – pravo ispitanika da zatraži da se obrada, izuzev pohrane, njegovih osobnih podataka obavlja isključivo uz njegov pristanak ili za potrebe uspostave, ostvarivanja ili obrane prava na sjedištu suda ili za zaštitu prava druge fizičke ili pravne osobe ili iz razloga javnog interesa EU-a ili države članice.

"Međunarodna organizacija" – organizacija i njezina podređena tijela uređena međunarodnim javnim pravom ili bilo koje drugo tijelo koje su sporazumom ili na osnovi sporazuma osnovale dvije ili više zemalja.

***"Automatizirani proces donošenja odluka"* –** obrada podataka koja za rezultat ima automatske odluke (bez ljudske intervencije) koje određuju pravne učinke ili imaju sličan učinak na podatke, uključujući profiliranje, kad to dovodi do donošenja odluke.

***"Profiliranje"* –** svaki oblik automatizirane obrade osobnih podataka koji se sastoji od upotrebe osobnih podataka za ocjenu određenih osobnih aspekata povezanih s pojedincem, posebno za analizu ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca.

***"Pseudonimizacija"* –** obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez upotrebe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi.

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

***"Izvršitelj obrade"* –** fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade

***"Glavni poslovni nastan"* –** a) što se tiče voditelja obrade s poslovnim nastanima u više od jedne države članice, mjesto njegove središnje uprave u EU-u, osim ako se odluke o svrhama i sredstvima obrade osobnih podataka donose u drugom poslovnom nastanu voditelja obrade u EU-u te je potonji poslovni nastan ovlašten provoditi takve odluke, u kojem se slučaju poslovni nastan u okviru kojeg se donose takve odluke treba smatrati glavnim poslovnim nastanom; b) što se tiče izvršitelja obrade s poslovnim nastanima u više od jedne države članice, mjesto njegove središnje uprave u EU-u ili ako izvršitelj obrade nema središnju upravu u EU-u, poslovni nastan izvršitelja obrade u EU u kojem se odvijaju glavne aktivnosti obrade u kontekstu aktivnosti poslovnog nastana izvršitelja obrade u mjeri u kojoj izvršitelj obrade podliježe posebnim obvezama u skladu s ovom Uredbom.

***"Treća strana"* –** fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade ni osobe koje su ovlaštene za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade

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

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

***"Prekogranična obrada"* –** bilo a) obrada osobnih podataka koja se odvija u EU-u u kontekstu aktivnosti poslovnih nastana u više od jedne države članice voditelja obrade ili izvršitelja obrade, a

voditelj obrade ili izvršitelj obrade imaju poslovni nastan u više od jedne države članice; ili b) obrada osobnih podataka koja se odvija u EU-u u kontekstu aktivnosti jedinog poslovnog nastana voditelja obrade ili izvršitelja obrade, ali koja bitno utječe ili je izgledno da će bitno utjecati na ispitanike u više od jedne države članice.
***"Povreda osobnih podataka"* –** kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili obrađeni na neki drugi način.

4. OSNOVNA NAČELA

Banka pridaje stratešku važnost zaštiti osobnih podataka fizičkih osoba s kojima surađuje (klijenti, suradnici, dobavljači itd.) pri čemu je svjesna da je svrha ove zaštite zaštititi osobe i druga temeljna prava slobode i ugleda.

Poštivanje prava i sloboda osoba predstavlja identifikacijski i vrijedan element za Banku, kako se to navodi u Etičkom kodeksu, u kojemu se navodi da: "zaštita sigurnosti naših klijenata, njihovih sredstava i povjerljivih informacija ne predstavlja samo jednu od naših temeljnih obveza, nego je ona temelj odnosa povjerenja koji želimo održavati s njima". U tu svrhu, Grupa se mora obvezati "na zaštitu osoba, njihovih sredstava i vrijednosti, njihovih podataka i internih organizacijskih procesa na takav način da pruža uslugu koja će u potpunosti zadovoljiti kriterije pouzdanosti, kontinuiteta i povjerljivosti"; jamčiti "stalno poštivanje zakona", osigurati "poštovanje kriterija potpune transparentnosti u informiranju klijenata o njihovim pravima na privatnost i o metodama kako postupamo s njihovim osobnim podacima".

U tu svrhu, Grupa primjenjuje model čiji je cilj osigurati da se osobni podaci:

- obrađuju zakonito, pošteno i transparentno u odnosu na ispitanika
- prikupljaju samo za specifične, eksplicitne i legitimne svrhe i da se daljnje ne obrađuju na način koji nije u skladu s tim svrhama (ograničenje svrhe)
- adekvatni, relevantni i ograničeni na ono što je potrebno za obradu (minimiziranje podataka)
- točni, i kad je to potrebno, ažurirani uz sve napore kako bi se brisali ili ispravili bez odgađanja, s obzirom na svrhu u koju se obrađuju
- moraju se čuvati u obliku u kojem se ispitanika može identificirati samo onoliko dugo koliko je potrebno u svrhu u koju su osobni podaci obrađeni (ograničenje čuvanja)
- moraju biti obrađeni na način koji osigurava odgovarajuću razinu sigurnosti, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja, korištenjem odgovarajućih tehničkih ili organizacijskih mjera (integritet i povjerljivost)

Upravljanje rizikom usklađenosti s obzirom na zaštitu osobnih podataka sastavni je dio sustava unutarnjih kontrola te se provodi kroz sve korporativne funkcije koje rade u sinergiji:

- Uprava, koja predstavlja voditelja obrade, zadužena je za utvrđivanje modela kontrola (sudionici, zaduženja, makroprocesi i informacijski tokovi) te osigurava njegov rad
- poslovne funkcije i funkcije podrške provode obradu utvrđujući unaprijed njenu svrhu i metode uz pomoć službenika za zaštitu podataka; oni poštuju procese i procedure, provjeravaju njihovu primjenu uz pomoć odgovarajućih kontrola prve razine, kako bi se u cijelosti i potpunosti poštivala važeća pravila i standardi ponašanja

- službenik za zaštitu podataka prati rizik usklađenosti, u skladu s pristupom temeljenim na procjeni rizika, u odnosu na zaštitu podataka, radeći samostalno kao specijalist funkcije praćenja usklađenosti u skladu sa Smjernicama o usklađenosti Grupe
- funkcija unutarnje revizije, kao dio svoje aktivnosti praćenja sustava unutarnje kontrole na trećoj razini, procjenjuje prikladnost i učinkovitost modela Grupe za upravljanje rizikom usklađenosti s obzirom na zaštitu privatnosti.

Svaka pojedina organizacijska struktura odgovorna je za obradu podataka te svaki pojedini zaposlenik, kao i suradnici društva, bez obzira na njihov ugovorni odnos, a općenitije govoreći svi oni koji provode obradu za koju ih je Banka ovlastila, u svojem svojstvu osoba ovlaštenih za obradu, moraju se pridržavati uputa koje im je Banka dala tijekom takve aktivnosti, poštujući povjerljivost i sigurnost obveza koje su propisane GDPR-om.

Obrada osobnih podataka koju provode osobe ovlaštene za obradu podataka mora se odnositi ili bilo u kojem slučaju biti povezana s funkcijama za koje su one povremeno zadužene kao dio organizacijske cjeline. Iz toga proizlazi da se svaki pojedini pristup osobnim podacima ostvaruje prilikom izvršavanja dodijeljenih zadataka ili na temelju zahtjeva ispitanika.

U tom smislu, programska podrška izrađuje se i primjenjuje na način koji osigurava pokretanje i ispravno funkcioniranje funkcija praćenja aktivnosti zaposlenika, klijenata i administratora sustava i to u skladu sa Sigurnosnim pravilima za praćenje poslovnih događaja.

Osim toga, Grupa uvijek usmjerava pažnju na korištenje tzv. Big Data, odnosno informatičkih resursa velikih količina, velike brzine i velike raznolikosti koji obuhvaćaju inovativne oblike analize i obrade podataka, osiguravajući poštivanje prava i sloboda ispitanika te usvajanje potrebnih mjera zaštite te, kad je to potrebno u skladu sa svrhom obrade, deidentifikacije.

Razmjena podataka unutar Grupe dopuštena je samo onoliko koliko je to zakonom dopušteno (npr. usklađenost sa zakonskim obvezama, izvršenje ugovora s ispitanikom, privola ispitanika).

Razmjena podataka izvan Grupe nije dopuštena ako ne predstavlja pravnu obvezu ili izvršenje ugovora.

5. ZADUŽENJA I ODGOVORNOSTI

5.1. Korporativna tijela

Korporativna tijela matičnoga društva odgovorna su, sukladno njihovim ovlastima i pravima, za osiguranje odgovarajućeg nadzora rizika neusklađenosti u pogledu zaštite osobnih podataka kojima je Grupa izložena ili bi mogla biti izložena.
Ovlasti korporativnih tijela opisane su u Statutu Banke, odgovarajućim propisima koji uređuju njihovo funkcioniranje, u Propisu o integriranom sustavu unutarnjih kontrola. Kad se spominju ti propisi, prikazuju se samo zadaci tijela koja su izravno povezana s temom ovih Smjernica.

5.1.1. Uprava

U vezi s praćenjem rizika nepoštovanja zaštite osobnih podataka, Uprava:

- odobrava model upravljanja rizikom nepoštovanja zaštite osobnih podataka (relevantne osobe, zaduženja, odgovornosti, makro-procese i tokove informacija) te, u tu svrhu, odobrava ovu Politiku
- imenuje Službenika za zaštitu podataka, određujući ga prema profesionalnim kvalitetama i vještinama, kao što su specijalizirano znanje o zakonodavstvu zaštite podataka i organizacijskoj strukturi društva
- prima informacije, najmanje jednom godišnje, od Službenika za zaštitu podataka o pitanjima zaštite podataka koja su od posebne važnosti.
- odmah se obavještava u slučaju problema važnih za poslovnu aktivnost a koji proizlaze iz kršenja povjerljivosti, raspoloživosti ili integriteta osobnih podataka
- analizira godišnja izvješća koja su izradile kontrolne funkcije društva

5.1.2. Nadzorni odbor

U pogledu praćenja rizika neusklađenosti u pogledu zaštite osobnih podataka, Nadzorni odbor, kao tijelo s kontrolnom funkcijom, nadzire poštovanje zakona, propisa i statuta te usklađenost s načelima ispravnog upravljanja.

Ako dođe do ozbiljnih problema koji proizlaze iz kršenja povjerljivosti, raspoloživosti ili integriteta osobnih podataka, o tome se Nadzorni odbor odmah izvješćuje te on analizira godišnja izvješća koja izrađuju kontrolne funkcije društva.

5.1.3. Odbor za rizike

U pogledu praćenja rizika neusklađenosti u pogledu zaštite osobnih podataka, Odbor za rizike podupire Nadzorni odbor kako bi se osigurala najbolja kontrola rizika glede neusklađenosti u pogledu zaštite osobnih podataka. Zadaci spomenuti u točki 5.1.1 prethodno se podnose na pažnju Odboru za upravljanje rizicima.

5.2. Službenik za zaštitu podataka

Službenik za zaštitu podataka savjetuje i prati usklađenost s GDPR-om u Banci, procjenjujući rizike svake obrade u pogledu prirode, opsega, konteksta i ciljeva obrade te utvrđujući procedure praćenja i s njim povezane kontrole.

S obzirom na propise o zaštiti osobnih podataka, Službenik za zaštitu podataka primjenjuje makroprocese funkcije praćenja usklađenosti navedene u Politici praćenja usklađenosti te metodologiju za procjenu rizika usklađenosti zajedno s Praćenjem usklađenosti.

Službenik za zaštitu podataka posebno je zadužen za sljedeće:
- provodi Politiku koje je odobrila Uprava
- osigurava provedbu modela nadzora zaštite osobnih podataka i provodi inicijative i intervencije potrebne za jamčenje njegove potpunosti, adekvatnosti, funkcionalnosti i pouzdanosti

- usvaja potrebne korektivne prilagodbe ili odgovarajuće intervenira u slučaju nedostataka ili slabosti u radu modela nadzora zaštite osobnih podataka
- pruža podršku poslovnim funkcijama i funkcijama podrške dajući mišljenje u slučaju povrede povjerljivosti podataka, dostupnosti ili integriteta osobnih podataka i daje informacije Upravi u slučaju ozbiljnih problema za poslovanje koji iz toga proizlaze
- pruža podršku poslovnim funkcijama u Procjeni utjecaja na privatnost (PIA) i davanje, ako se to zatraži, svojeg mišljenja o istoj te praćenje njezine izvedbe
- pruža podršku poslovnim funkcijama u procjeni događaja koji se mogu smatrati povredom osobnih podataka, informira AZOP o istoj i/ili ispitanika
- najmanje jednom godišnje obavještava Upravu o pitanjima zaštite osobnih podataka koja su od posebne važnosti
- informira i upoznaje zaposlenike o obvezama koje proizlaze iz Uredbe i drugih odredbi o zaštiti podataka
- surađuje s AZOP-om i djeluje kao kontakt osoba za AZOP na bilo kojem pitanju vezanom za obradu, uključujući prethodno savjetovanje nakon Procjene utjecaja na privatnost (PIA)
- daje savjete operativnim ili poslovnim funkcijama koje se odnose na bilo koju aktivnost vezanu uz obradu osobnih podataka
- provodi test ravnoteže legitimnog interesa voditelja obrade
- upravlja povratnim informacijama AZOP-u i ispitanicima nakon žalbi, izvješća ili pritužbi podnesenih nadležnom tijelu i obrađuje zahtjeve za ostvarivanje prava ispitanika
- ocjenjuje kontrole prve razine predložene od strane operativnih ili poslovnih funkcija i definira, u suradnji s Praćenjem usklađenosti, kontrole druge razine u pogledu zaštite osobnih podataka, utvrđuje njihove ciljeve, učestalost i način izvršenja
- provodi kontrole druge razine na području zaštite osobnih podataka
- uspostavlja i održava Evidenciju aktivnosti obrade u suradnji s operativnim i poslovnim odjelima
- barem jednom godišnje potvrđuje usklađenost ovog dokumenta s referentnim zakonima i internim propisima te predlaže ažuriranja uz podršku Organizacije
- predlaže organizacijske i proceduralne promjene s ciljem osiguranja odgovarajućeg praćenja rizika neusklađenosti
- obavlja zadatak usmjeravanje, koordinacije i kontrole društava Grupe, koja nisu pod centraliziranom upravom, u području zaštite osobnih podataka, pružajući specijalističku podršku lokalnim strukturama onih koja su osnovana na području Europske unije te, na zahtjev, u odnosima s nadzornim tijelima.

Službenik za zaštitu podataka utvrđuje se u Praćenju usklađenosti, a odgovoran je izravno korporativnim tijelima.
Neovisnost Službenika za zaštitu podataka vidi se u tome što se on ne može ukloniti s radnog mjesta ni kazniti zbog ispunjavanja zadataka, pri čemu se u vrijeme njegovog imenovanja utvrđuje prikladan proračun troškova te njegovi zadaci kao dio ove Politike i Procedura .

5.3. Glavne korporativne funkcije u opsegu GDPR-a

5.3.1. Praćenje usklađenosti

U skladu sa Smjernicama o usklađenosti, Praćenje usklađenosti:

- utvrđuje, u suradnji sa Službenikom za zaštitu podataka, metode procjene rizika neusklađenosti u pogledu zaštite osobnih podataka i postupke za ublažavanje tog rizika

- pruža podršku Službeniku za zaštitu podataka pri utvrđivanju kontrola druge razine
- na temelju periodičnih izvješća i drugih tokova informacija Službenika za zaštitu podataka, drugih korporativnih funkcija te izravne provjere daje neovisnu procjenu rizika neusklađenosti s propisima o zaštiti osobnih podataka i adekvatnosti mjera zaštite postavljenih u svrhu izbjegavanja rizika i, ako se ukaže potreba, zahtijeva od Službenika za zaštitu podataka odgovarajuće postupke kako bi ojačali te mjere zaštite
- u okviru periodičnih izvješća o adekvatnosti praćenja usklađenosti koja se podnose korporativnim tijelima, pruža cjelovite i sveobuhvatne informacije o područjima koja predstavljaju najveći rizik, a kojima upravljaju zasebne funkcije, uključujući propise o zaštiti osobnih podataka

5.3.2. Upravljanje rizicima

U pogledu upravljanja rizikom neusklađenosti u pogledu zaštite osobnih podataka, Upravljanje rizicima surađuje sa Službenikom za praćenje usklađenosti i Službenikom za zaštitu podataka kako bi utvrdilo metode procjene rizika neusklađenosti, potičući sinergiju s alatima i metodama Službenika za praćenje operativnog i reputacijskog rizika.

5.3.3. Unutarnja revizija

Unutarnja revizija, u kontekstu svoje aktivnosti nadzora nad cjelokupnim sustavom internih kontrola, povremeno procjenjuje potpunost, adekvatnost, funkcionalnost (u smislu učinkovitosti i djelotvornosti) te pouzdanost modela upravljanja rizikom neusklađenosti Grupe te surađuje sa Službenikom za praćenje usklađenosti koji je zadužen za kontrolu toga rizika, kako bi se provjerila učinkovita primjena unutarnjih i vanjskih propisa u Grupi te upravljanje bilo kakvim nedostatcima koji su se pojavili tijekom provjera.
Nakon provedenih provjera i procjena, Unutarnja revizija izvješćuje o svim nepravilnostima vezanim uz obradu osobnih podataka nadležnim korporativnim tijelima te Službeniku za zaštitu podataka te o tome izvješćuje Upravu.

5.3.4. Pravni poslovi

Pravni poslovi u svezi s regulativom za zaštitu osobnih podataka:
- podupiru Službenika za zaštitu podataka pri trajnom utvrđivanju primjenjivih zakonskih odredbi, praćenju njihovih izmjena, uključujući također sudsku praksu i njezino tumačenje
- podržavaju Službenika za zaštitu podataka pri provođenju testa ravnoteže kako bi se utvrdila pravna osnova legitimnog interesa
- podržavaju Službenika za zaštitu podataka u identificiranju mjera koje doprinose osiguranju zakonitosti obrade u procesu procjene učinka na privatnost (PIA)
- uz podršku Službenika za zaštitu podataka utvrđuju uvjete pohrane osobnih podataka
- podupiru Službenika za zaštitu podataka u vezi s pravnim aspektima koji se odnose na ugovorne odredbe, obrasce, komunikaciju s korisnicima ili ispitivanje značajnih slučajeva otkrivenih nepravilnosti

Pravni poslovi također upravljaju sudskim i administrativnim sporovima vezanim uz eventualne povrede odredbi od strane Banke te o istom informiraju relevantna korporativna tijela.

5.3.5. *Organizacija*

U pogledu upravljanja rizikom neusklađenosti u pogledu zaštite osobnih podataka Organizacija, u dogovoru sa Službenikom za zaštitu podataka:

- utvrđuje organizacijska rješenja u skladu s ciljevima i Politikom o zaštiti osobnih podataka. Naročito, nadgleda analizu i usvajanje procesa promjene i organizacijskih promjena i razvoja, koji također proizlaze iz regulatornih obveza vezanih uz zaštitu osobnih podataka
- kontinuirano osigurava da se zadaci i odgovornosti u vezi sa zaštitom osobnih podataka rasporede na jasan i primjeren način, osiguravajući da organizacija bude u skladu s načelima Politike o integriranom sustavu unutarnjih kontrola
- pruža podršku Službeniku za zaštitu podataka u ažuriranju ovih Smjernica, odobravajući ili odbacujući predložene uloge i odgovornosti.

5.3.6. *Poslovne funkcije i funkcije podrške*

Poslovne funkcije i funkcije podrške Banke i sektora odgovorne su za proces upravljanja rizicima neusklađenosti u pogledu zaštite osobnih podataka.
One se pridržavaju korporativnih procesa i procedura, provjeravaju njihovu primjenu uz odgovarajuće kontrole prve razine kako bi se osiguralo ispravno provođenje aktivnosti s ciljem potpunog i cjelovitog poštivanja važećih pravila i standarda ponašanja. Kontrole prve razine u pogledu zaštite osobnih podataka, koje utvrde poslovne funkcije i funkcije podrške, ispituje Službenik za zaštitu podataka, koji procjenjuje jesu li one zaista sposobne postići zadane ciljeve kontrole te, kad je to potrebno, on zahtijeva da se takve kontrole pojačaju. Kad poslovne funkcije i funkcije podrške utvrde kritične probleme, izravno ili ako na njih ukažu nadležne funkcije kontrole druge ili treće razine u društvu, poslovne funkcije i funkcije podrške poduzimaju aktivnosti koje su potrebne za rješavanje problema.

Posebno, te poslovne funkcije i funkcije podrške:

- igraju aktivnu ulogu pri ispunjavanju formalnosti propisanih regulativom o zaštiti osobnih podataka koje su propisane posebnim smjernicama, unutarnjim procesima i procedurama
- osiguravaju, uz podršku Službenika za zaštitu podataka, tehničku zaštitu podataka i integriranu zaštitu podataka, definiranje ciljeva, sredstava i sigurnosnih mjera za obradu osobnih podataka te, po potrebi, vode Procjene utjecaja na privatnost (PIA)
- uključuju Službenika za zaštitu podataka tako da i) on utvrđuje subjektivnu ulogu koja se dodjeljuje dobavljaču/trećoj strani te eventualnim pod-dobavljačima, ako je za to ovlašten i ii) procjenjuje u slučaju da je dobavljač/treća strana osnovana ili posluje izvan područja Europske unije, postoje li neophodne mjere zaštite
- u slučaju kad poslovne funkcije i funkcije podrške sklapaju ugovore s dobavljačima/trećim stranama:
    - finaliziraju, uz pomoć Pravnih poslova i Službenika za zaštitu podataka, akt o imenovanju za izvršitelja obrade te ugovor ili drugi pravni akt u slučaju imenovanja voditelja obrade
    - formaliziraju ugovorne uvjete koji su potrebni za prijenos osobnih podataka izvan teritorija Europske unije koje utvrde Službenik za zaštitu podataka i Pravni poslovi
- pomažu kako bi se programi za obrazovanje o zaštiti osobnih podataka ispravnije implementirali
- dužni su obavijestiti Službenika za zaštitu podataka o svim situacijama ili događajima nepoštivanja propisa koji uređuju zaštitu osobnih podataka za koje saznaju.

5.3.7. Centralna nabava

S ciljem praćenja rizika neusklađenosti u pogledu zaštite osobnih podataka Centralna nabava:

- finalizira, uz pomoć Pravnih poslova i Službenika za zaštitu podataka, imenovanje izvršitelja obrade te ugovor ili drugi pravni akt u slučaju imenovanja zajedničkih voditelja obrade
- formaliziraju ugovorne uvjete koji su potrebni za prijenos osobnih podataka izvan teritorija Europske unije koje utvrde Službenik za zaštitu podataka i Pravni poslovi

5.3.8. Ljudski resursi i Organizacija

S ciljem praćenja rizika neusklađenosti u pogledu zaštite osobnih podataka, Ljudski resursi i Organizacija:

- pružaju podršku Službeniku za zaštitu podataka pri razvoju inicijativa usmjerenih na širenje, na svim razinama Banke, korporativne kulture u pogledu privatnosti i povećanja razine svijesti o povezanim rizicima
- surađuju sa Službenikom za zaštitu podataka pri definiranju i provođenju radionica i treninga u području zaštite osobnih podataka

S ciljem praćenja rizika neusklađenosti u pogledu zaštite osobnih podataka, Ljudski resursi i Organizacija igraju aktivnu ulogu pri provođenju disciplinskih mjera prema zaposlenicima koji su prijavljeni za nepravilnosti pri radu, provođenjem sljedećih aktivnosti:

- procjenjuju i promiču disciplinske mjere prema onim zaposlenicima koji su prijavljeni za nepravilnosti pri radu s obzirom na obveze iz propisa o zaštiti osobnih podataka
- procjenjuju primjenjivost mjera zaštite koje su nametnute sporazumima o kolektivnom pregovaranju za zaposlenike kojima su izrečene kaznene, građanske i upravne mjere za navodno kršenje propisa o zaštiti osobnih podataka

5.3.9. Informacijska i komunikacijska tehnologija

S ciljem praćenja rizika neusklađenosti u pogledu zaštite osobnih podataka, Informacijska i komunikacijska tehnologija zadužena je za:

- provedbu odgovarajućih tehničkih mjera, identificiranih uz potporu Službenika za zaštitu podataka
- pružanje podrške Službeniku za zaštitu podataka pri identifikaciji područja primjene aplikacija koja mogu imati utjecaj na obradu osobnih podataka
- uključivanje Službenika za zaštitu podataka u slučaju IT intervencija ili razvoja aplikacija ili softvera koji mogu utjecati na obradu osobnih podataka u svrhu procjene mogućeg utjecaja na privatnost
- izvršenje korektivnih mjera koje je prijavio Službenik za zaštitu podataka.

5.3.10. Korporativna sigurnost

S ciljem praćenja rizika neusklađenosti u pogledu osobnih podataka, Korporativna sigurnost zadužena je za:

- utvrđivanje, uz pomoć Službenika za zaštitu podataka, pravila i mjera za zaštitu podataka, informacija i infrastrukture kako bi se održali sigurnosni uvjeti u skladu s važećim propisima

- sudjelovanje u procjeni utjecaja privatnosti na identifikaciju i definiranje sigurnosnih mjera koje se primjenjuju na obradu osobnih podataka
- uključivanje Službenika za zaštitu podataka u slučaju sigurnosnih događaja koji se tiču osobnih podataka radi utvrđivanja povrede osobnih podataka koji će biti prijavljeni AZOP-u i/ili biti dostavljeni ispitaniku, kao i pripremu korektivnih mjera usmjerenih na rješavanje takvih situacija
- pruža podršku, iz sigurnosnih aspekata, poslovnim funkcijama i funkcijama podrške pri utvrđivanju tehničkih i organizacijskih mjera za osiguranje razine praćenja koja je primjerena rizičnom profilu obrade

6. MAKROPROCESI ZAŠTITE OSOBNIH PODATAKA

Utvrđeni su sljedeći glavni makro-procesi koji opisuju postupke za nadgledanje i praćenje zakona koji se odnose na zaštitu osobnih podataka:

1. identifikacija obrada
2. definicija metoda obrade i sigurnosnih mjera (tehnička zaštita podataka)
3. brisanje podataka
4. upravljanje neusklađenostima
5. informiranje ispitanika i dobivanje privola
6. upravljanje pravima ispitanika
7. naknadna provjera
8. širenje korporativne kulture primjerenog upravljanja osobnim podacima
9. suradnja s tijelima vlasti.

6.1. Identifikacija obrada

Identifikacija i evidentiranje obrada osobnih podataka koje se provode ili za koje se pretpostavlja da se provode predstavljaju primarnu aktivnost u svrhu primjene i usklađenosti sa regulativom vezanom za zaštitu osobnih podataka.

Poslovne funkcije i funkcije podrške, uz pomoć Službenika za zaštitu podataka, identificiraju pojedinačne obrade, svrhe obrada, ulogu sudionika i kategorije primatelja kojima se podaci otkrivaju ili mogu otkriti.

Postupke koji se provode bilježe poslovne funkcije i funkcije u posebnom registru čiji je voditelj Službenik za zaštitu podataka, a koji sadrži podatke propisane Uredbom i ažurira se najmanje jednom godišnje.

6.2. Definicija metoda obrade i sigurnosnih mjera (tehnička zaštita podataka - privacy by design)

Ovaj makro-proces usmjeren je na definiranje - imajući na umu prirodu , opseg, kontekst i svrhu obrada, kao i rizike za prava i slobode fizičkih osoba, odgovarajuće mjere kako bi se osiguralo da se obrade provode u skladu sa svrhom za koju su prikupljeni i GDPR-om.

Naročito, poslovne funkcije i funkcije podrške koje predlažu novu obradu surađuju sa Službenikom za zaštitu podataka kako bi utvrdile – upravo iz faze dizajna pa sve do kraja ciklusa obrade – rizike usklađenosti te prikladne tehničke i organizacijske mjere u svrhu ublažavanja rizika te očuvanja obrađenih osobnih podataka. Posljedično, ta je aktivnost sastavni dio korporativnih procesa, kao i dizajna, izrade i arhitekture informacijskih sustava.

U tu bi svrhu poslovne funkcije i funkcije podrške:

- provjeravaju zakonitost obrade, koristeći metode navedene u točki 6.2.1., uz podršku Službenika za zaštitu podataka te, ako je potrebno, Pravnih poslova
- osiguravaju, uz podršku Službenika za zaštitu podataka, da se prema zadanim postavkama obrađuju samo osobni podaci potrebni za svaku pojedinačnu svrhu (načelo minimizacije)
- provjeravaju uz podršku Službenika za zaštitu podataka, postoji li vjerojatnost da obrada predstavlja visok rizik za prava i slobode ispitanika te pokreću, ako je potrebno, proces procjene utjecaja na privatnost (vidi točku 6.2.3.)
- provjeravaju uključenost trećih strana i traže od Službenika za zaštitu podataka da procijeni ulogu koju treba dodijeliti trećim stranama (voditelj, izvršitelj, zajednički voditelj) (vidi točku 6.2.2.)
- utvrđuju eventualne potrebe za prijenos podataka izvan EU-a te zahtijevaju od Službenika za zaštitu podataka utvrđivanje odgovarajućih zaštitnih mjera (vidi točku 6.2.2.)
- utvrđuju, uz potporu nadležnih korporativnih struktura (posebice Informacijske i komunikacijske tehnologije, Korporativne sigurnosti te Službenika za zaštitu podataka), tehničke i organizacijske mjere kako bi se osigurala odgovarajuća razina pokrivenosti za profil rizika obrada.

Procjene i donesene odluke dokumentira i pohranjuje Službenik za zaštitu podataka kako bi pokazao poštovanje načela odgovornosti.

Poslovna funkcija ili funkcija podrške pokreće makro-proces u slučajevima:

- razvoja novih proizvoda ili usluga ili njihovih bitnih promjena, uključujući potrebne IT intervencije (softverske i hardverske) (sukladno internim propisima o novim proizvodima, uslugama, pokretanju novih aktivnosti i ulasku na nova tržišta)
- značajnih projektnih inicijativa (u skladu s internim propisima koji se odnose na upravljanje projektnim inicijativama)
- inicijative za eksternalizaciju (sukladno internim propisima koji se odnose na eksternalizaciju)
- tehnološke promjene (npr. značajne promjene tehnoloških rješenja ili nadogradnje u verziji koje mogu utjecati na postojeće obrade, u skladu s internim propisima o upravljanju promjenama)
- organizacijskih promjena (npr. korporacijska reorganizacija i značajne izmjene procesa)
- korporacijskih transakcija (npr. akvizicije ili prodaje)
- primjene Big Data
- bilo kojem drugom slučaju pokretanja ili izmjene obrade osobnih podataka.

6.2.1. Provjera zakonitosti obrade

Radi utvrđivanja zakonitosti obrade, poslovna funkcija i funkcija podrške, uz pomoć Službenika za zaštitu podataka i, ako je potrebno, Pravnih poslova, utvrđuje pravnu osnovu postupanja između:

- privole
- izvršenja ugovora u kojem je ispitanik stranka ili izvršenje predugovornih mjera usvojenih na zahtjev ispitanika

- zakonske obveze kojima Banka podliježe
- legitimnog interesa voditelja obrade ili trećih strana kojima se dostavljaju podaci, pod uvjetom da interesi ili prava i temeljne slobode ispitanika ne prevladavaju.

Obrada koja se provodi radi legitimnog interesa voditelja obrade ne zahtijeva privolu, no zahtijeva da se ispitaniku precizno navedu razlozi zbog kojih se to smatra opravdanim interesom voditelja obrade.
Kako bi se utvrdilo može li se obrada smatrati legitimnim interesom, Službenik za zaštitu podataka, uz potporu Pravnih poslova, provodi takozvani „test ravnoteže“, odnosno ocjenjuje:

- da je obrada dovoljno specifična da jasno naglasi interes voditelja obrade u odnosu na prava ispitanika (npr. kada postoji sumnja na prijevaru na štetu Banke)
- da je obrada neophodna za ostvarivanje temeljnog prava ili se obavlja u javnom interesu, uzimajući u obzir moguću štetu koja bi nastala za Banku ako ne provede obradu (primjerice, u slučaju video nadzora iz sigurnosnih razloga)
- da je obrada unutar razumnog očekivanja ispitanika (npr. obrade radi prevencije prijevara)
- postojanje legitimnog interesa kada postoji odnos između ispitanika i voditelja obrade (npr. kada je ispitanik klijent ili zaposlenik voditelja obrade), a ispitanik može razumno očekivati da će se podaci obraditi u svrhu za koju su prikupljeni.

Postupak koji se može pripisati automatiziranom postupku donošenja odluka zakonit je ako je:

- neophodan za izvršenje ugovora ili u svrhu sklapanja ugovora u kojemu je ispitanik jedna od strana
- dopušten zakonom EU-a ili države članice koji mora poštivati voditelj obrada, koji također određuje odgovarajuće mjere za zaštitu prava, sloboda i legitimnih interesa ispitanika
- temeljen na izričitoj privoli ispitanika.

Ako obrada uključuje korištenje određenih kategorija podataka (npr. podaci koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatima, kao i genetski podaci, biometrijski podaci namijenjeni jednoznačnoj identifikaciji fizičke osobe, podaci koji se odnose na zdravlje, seksualni život ili seksualnu orijentaciju osobe) privola ispitanika je obvezna, osim ako:

- su podaci neophodni za ispunjavanje obveza i ostvarivanje posebnih prava voditelja obrade ili ispitanika na području radnoga prava, sigurnosti i socijalne zaštite, u onoj mjeri u kojoj je to dopušteno važećim zakonom ili kolektivnim ugovorom
- se odnosi na osobne podatke koje je ispitanik javno objavio
- je potrebno utvrditi, ostvarivati ili braniti pravo na sudu
- je neophodno iz razloga značajnog javnog interesa na temelju prava EU-a ili država članica
- je neophodno za potrebe arhiviranja u javnom interesu, za znanstvena ili povijesna istraživanja ili za statističke svrhe na temelju EU-a ili nacionalnog prava.

Ovisno o karakteristikama obrade i pravne osnove koja ju legitimira, Službenik za zaštitu podataka provjerava da su ispitaniku pružene potrebne informacije, da su od ispitanika zatražene potrebne privole (vidi točku 6.5.) te da ispitanik može ostvariti svoja zakonska prava (vidi točku 6.6.); primjerice u slučaju obrade koja uključuje proces automatiziranog odlučivanja, pravo na ljudsku intervenciju, izražavanje mišljenja, dobivanje objašnjenja donesene odluke ili osporavanje odluke.

6.2.2. Upravljanje odnosima s trećim stranama i prijenos podataka izvan EU-a

Što se tiče obrade osobnih podataka koje Banka povjerava trećim osobama (uključujući dobavljače/ treće strane i eventualne pod-dobavljače, obično u okviru raznih ugovora i odnosa suradnje, osim voditelja obrade utvrđuju se zajednički voditelj obrade i izvršitelj obrade.

Prije sklapanja ugovora ili suradnje s trećom stranom koja bi mogla dovesti do obrade podataka, poslovne funkcije i funkcije podrške zahtijevaju od Službenika za zaštitu podataka procjenu uloge treće strane (voditelj obrade, zajednički voditelj obrade, izvršitelj obrade).

Ako je treća strana utvrđena kao izvršitelj obrade, Centralna nabava ili poslovna funkcija ili funkcija podrške – kad je to primjenjivo, formalizira to ulogu putem posebnog akta o imenovanju, čiji se tekst utvrđuje uz pomoć Pravnih poslova i Službenika za zaštitu podatka.

Izvršitelj obrade ne smije podugovarati usluge s trećim stranama, u cijelosti ili djelomično, bez prethodne pisane suglasnosti Banke u kojoj se navodi da je izvršitelj obrade dužan provjeriti pravilno ispunjenje svih obveza od strane poddobavljača te da je izvršitelj odgovaran u slučaju neispunjavanja obveza od strane poddobavljača. Pri davanju suglasnosti za podugovaranje, Banka provjerava daje li izvršitelj jamstvo pravilnog izvođenja svih zakonskih obveza od strane potencijalnog podizvođača, posjedovanje dozvola, odobrenja i certifikata potrebnih za provedbu ugovora te njegovu tehničku, profesionalnu i financijsku prikladnost.

U slučaju partnerstva s trećim stranama ili članicama PBZ Grupe koje dovodi do zajedničkog utvrđivanje ciljeva i način obrade osobnih podataka, te ugovorne strane nastupaju kao zajednički voditelji obrade. U tom slučaju, Pravni poslovi definiraju posebne klauzule u ugovoru o suradnji radi reguliranja uloga zajedničkih voditelja obrade.

Nakon određivanja uloge treće strane, poslovna funkcija ili funkcija podrške, uz pomoć Službenika za zaštitu podataka, ažurira Evidenciju aktivnosti obrade (vidi točku 6.1.).

U slučaju kad je treća strana osnovana ili posluje izvan Europske unije, poslovna funkcija ili funkcija podrške, prije sklapanja ugovora ili dodjele zadatka o suradnji, koji može uključivati prijenos osobnih podataka, zahtijeva od Službenika za zaštitu podataka da procijeni postoje li odgovarajuće zaštitne mjere. Službenik za zaštitu podataka provjerava prenose li se podaci u skladu sa zakonom, svrhom obrade te, kad je potrebno, postoje li privole ispitanika, te utvrđuje uz pomoć Pravnih poslova s tim povezane ugovorne metode i uvjete.

6.2.3. Procjena utjecaja na privatnost (PIA)

Ako je procjena potencijalnih rizika obrade „visok rizik“ za prava i slobode fizičkih osoba, u svim slučajevima utvrđenim Uredbom ili nadzornim tijelima, poslovne funkcije ili funkcije podrške, u suradnji sa Službenikom za zaštitu podataka, prije nastavka obrade, moraju napraviti procjenu utjecaja obrade na zaštitu osobnih podataka (tzv. Procjena utjecaja na privatnost – engl. Privacy Impact Assessment – PIA, u daljnjem tekstu: PIA) kako bi se definirale odgovarajuće tehničke i organizacijske sigurnosne mjere.

Ako izvršitelj obrade provodi obradu u cijelosti ili djelomično, Procjena utjecaja na privatnost provodi se uz pomoć izvršitelja koji mora pružiti sve potrebne informacije.

Rezultat Procjene utjecaja na privatnost daje su u posebnom izvješću koje sadrži informacije propisane Uredbom.

U slučaju obrade visokog rizika i u nedostatku posebnih mjera za ublažavanje navedenog rizika, poslovna funkcija ili funkcija podrške, nakon savjetovanja sa Službenikom za zaštitu podataka, odlučuje ili a) da neće započeti s obradom podataka ili da će, u slučaju da je ista već započela, istu zaustaviti ili b) će se prethodno savjetovati s nadzornim tijelom u kojem slučaju će Službenik za zaštitu podataka službenim putem poslati zahtjev nadzornom tijelu, kojem zahtjevu će priložiti izvješće o obavljenoj Procjeni utjecaja na privatnost. Nadzorno tijelo dužno je u roku od osam tjedana dostaviti pisano mišljenje, temeljem kojeg poslovna funkcija ili funkcija podrške, uz potporu Službenika za zaštitu podataka, radnje koje će se provesti kako bi se nastavilo s obradom ili, alternativno, ako se ne može pridržavati naputaka koje je predložilo nadležno tijelo, odlučiti da neće pokrenuti obradu ili da će blokirati postojeću obradu.

Službenik za zaštitu podataka obavlja periodički pregled svih visokorizičnih aktivnosti obrada, provodeći za njih Procjenu utjecaja na privatnost s različitom učestalošću, a ovisno o vrsti obrade i rizika za prava i slobode ispitanika.

6.3. Brisanje podataka

Cilj procesa je osigurati da se podaci čuvaju u obliku koji omogućuje identifikaciju ispitanika za razdoblje ne dulje od onog potrebnog za ostvarenje svrhe za koju su podaci prikupljeni, nakon čega moraju biti izbrisani ili anonimizirani.

U tu svrhu, Pravni poslovi, uz potporu Službenika za zaštitu podataka, određuju temeljem relevantnih zakonskih odredbi razdoblje maksimalnog čuvanja za svaku vrstu obrade (vidi točku 6.2.1.). U slučaju novih obrada ova se procjena provodi u postupku tehničke zaštite podataka i integrirane zaštite podataka (vidi točku 6.2.), a vrijeme čuvanja bilježi se u Evidenciji aktivnosti obrada(vidi točku 6.1.).

Banka obrađuje osobne podatke dok za to postoji svrha, nakon čega se pohranjuju sukladno važećoj regulativi. Jednom kada je ostvarena svrha obrade, podaci se pohranjuju u odvojenu arhivu, pristup kojoj imaju samo funkcije kojima je ovlaštenje za pristup dao Službenik za zaštitu podataka (primjerice Unutarnja revizija i Pravni poslovi), uz istovremenu njihovu deidentifikaciju ili brisanje iz aplikacija. Ako je stvaranje odvojene arhive tehnički presloženo ili preskupo, podaci mogu ostati u aplikacijama s limitiranim pristupom samo ovlaštenim funkcijama.

Službenik za zaštitu podataka, putem indikacija iz Evidencije aktivnosti obrada, prati istek zakonskih rokova čuvanja te provjerava provođenje potrebnih mjera za odvajanje.

6.4. Plan postupanja u slučaju neusklađenosti

Službenik za zaštitu podataka upravlja slučajevima neusklađenosti, pruža podršku i surađuje s odjelom u kojem se isti dogodio, da bi se osiguralo određivanje i provedba mjera koje treba poduzeti kako bi se uklonili ili smanjili učinci neusklađenosti te riješili organizacijski i/ili proceduralni nedostatci.

Poslovne funkcije i funkcije potpore pružaju podršku te surađuju sa Službenikom za zaštitu podataka pri upravljanju slučajevima neusklađenosti, osiguravajući određivanje i provođenje neophodnih korektivnih mjera.

Ukoliko slučaj neusklađenosti predstavlja povredu osobnih podataka, primjerice sigurnosni incident koji predstavlja povredu povjerljivosti, dostupnosti ili integriteta osobnih podataka Službenik za zaštitu osobnih podataka procjenjuje koliki je njegov utjecaj na rizik za prava i slobode fizičkih osoba, a radi obveze obavještavanja nadzornog tijela odnosno ispitanika.

Upravljanje događajem povrede osobnih podataka dio je širega procesa upravljanja kritičnim događajima, kako to propisuju posebni interni akti. Naročito, Službenik za zaštitu podataka, koristeći strukturu odgovornu za upravljanje kritičnim događajima, utvrđuje i kvalificira rizike i štetu povezanu s povredom osobnih podataka i procjenjuje njihov opseg.

U slučaju utvrđenja povrede osobnih podataka, Službenik za zaštitu podataka dužan je u roku od 72 sata od trenutka kada je voditelj obrade saznao za povredu obavijestiti AZOP, osim ako nije vjerojatno da predmetna povreda predstavlja postojanje rizika za prava i slobode fizičke osobe. Ako je rizik visok, Službenik za zaštitu podataka mora informirati i ispitanike te im dati precizne informacije o radnjama koje preporučuje Banka kako bi se zaštitili od povrede.

Pozivanje na prava i slobode ispitanika prvenstveno se odnosi na kršenje regulative koja se tiče prava na privatnost (npr. gubitak kontrole nad osobnim podacima, diskriminaciju, krađu identiteta, financijske gubitke, narušavanje ugleda, kršenje povjerljivosti, ili bilo kakvu drugu značajnu ekonomsku ili socijalnu štetu za dotičnu osobu), ali može se odnositi i na druga temeljna prava, kao što su sloboda izražavanja i misli ili sloboda kretanja.

Ako su ispitanici uključeni u povredu osobnih podataka iz više od jedne države članice EU-a te ako je uključeno više voditelja obrade, Službenik za zaštitu podataka o povredi obavještava vodeće nadzorno tijelo (koje je istovremeno nadzorno tijelo u glavnom poslovnom nastanu), navodeći države u kojima su smješteni poslovni nastani i fizičke osobe koje su potencijalno ili stvarno uključene u problem.

Ako povreda uključuje više voditelja obrade, svaki od njih obavijestit će lokalno nadzorno tijelo. Službenika za zaštitu podataka informira se o povredi do koje je došlo i o protumjerama koje su usvojene kako bi se utvrdio utjecaj na razini Grupe.

Za svaku povredu osobnih podataka, bez obzira na to što je nadležno tijelo obaviješteno, Službenik za zaštitu podataka vodi registar kritičnih događaja u kojem dokumentira povrede osobnih podataka, posljedice, postupke za ublažavanje te, ako je potrebno, razloge neuspjeha obavješćivanja. Registar je dostupan nadzornom tijelu u slučaju istrage.

6.5. *Informiranje ispitanika te pribavljanje privola*

Cilj procesa je prenijeti ispitanicima sve potrebne informacije kako bi se osigurala poštena i transparentna obrada, napisane na sažet, jasan, razumljiv, lako dostupan način i jednostavnim i jasnim rječnikom.
Iz tih razloga, Službenik za zaštitu podataka izrađuje, uz pomoć Pravnih poslova, obavijest s općim informacijama i relevantne privole za svaku vrstu ispitanika čiji se podaci obrađuju (npr. klijenti, potencijalni klijenti, zaposlenici itd.), kao i obavijest s posebnim informacijama i relevantne privole, i to svaki put kad je to potrebno za novu posebnu obradu koja se utvrdi metodama obrade i sigurnosnim mjerama (vidi točku 6.2).

Pri izradi informacije i privole zaposlenika uključuju se također i Ljudski resursi i organizacija.

Obavijest s informacijama koja se izrađuje na temelju procjene pri utvrđivanju metoda obrade i sigurnosnih mjera:

- dostavlja se ispitaniku u pisanom obliku (ili u elektroničkom formatu, u slučaju online usluga) u trenutku pribavljanja osobnih podataka, pod uvjetom da se podaci prikupljaju izravno od ispitanika (npr. pri uspostavljanju poslovnog odnosa s bankom)
- umjesto toga, ako se podaci ne prikupljaju izravno od ispitanika:
    - informacija se dostavlja u razumnom roku, no ipak najkasnije za jedan mjesec, nakon pribavljanja osobnih podataka
    - ako se osobni podaci koriste za komunikaciju s ispitanikom, informacija se dostavlja najkasnije do trenutka kad se ostvari prva komunikacija s ispitanikom
    - ako se predviđa otkrivanje podataka drugim primateljima, informacija se dostavlja najkasnije do trenutka kad se osobni podaci prvi put otkriju

Informacija se ne dostavlja ispitaniku ako i u onoj mjeri do koje:

- ispitanik već ima tu informaciju
- dostava takve informacije je nemoguća ili bi zahtijevala nerazmjeran napor
- pribavljanje ili objava informacija izričito se propisuje zakonom države članica EU-a kojemu podliježe voditelj obrade
- osobni podaci moraju ostati tajni zbog obveze profesionalne povjerljivosti ili tajne što se propisuje zakonom EU-a ili države članice EU-a

Na temelju procjene izrađene u prethodno navedenom procesu utvrđivanja metoda i sigurnosnih mjera, osim navedenoga, Službenik za zaštitu podataka osigurava, uz pomoć Pravnih poslova, obrazac privole koji je potreban kako bi se osigurala zakonitost obrade.

Privole prikupljene prije izdavanja ove Politike ostaju na snazi ako obuhvaćaju sve elemente navedene u prethodnom tekstu.

6.6. *Upravljanje pravima ispitanika*

Cilj je ovog postupka jamčiti ispitanicima učinkovito ostvarivanje prava ispitanika uređenih Propisom:

a) pravo pristupa, tj. pravo na dobivanje potvrde o tome obrađuju li se osobni podaci ili ne, te ako se obrađuju, pravo na dobivanje pristupa podacima ili kopijama

b) pravo ispravljanja/integracije obrađenih podataka kako bi se zajamčilo da su uvijek točni i ažurni
c) pravo na brisanje osobnih podataka koji se obrađuju
d) pravo na ograničenje obrade za potrebe zaštite prava ispitanika
e) pravo na prijenos podataka, tj. pravo na:
    1. primitak osobnih podataka koje Banka obrađuje i čuvanje istih za daljnju upotrebu u osobne svrhe
    2. prijenos osobnih podataka drugom voditelju obrade
f) pravo na protivljenje obradi na temelju legitimnog interesa voditelja obrade
g) pravo povlačenja privole koje se mora moći ostvariti jednako jednostavno kao i davanje privole
h) pravo na ljudsku intervenciju, izražavanje mišljenja, dobivanje objašnjenja o donesenoj odluci i osporavanje te odluke u slučajevima donošenja odluke isključivo automatiziranom odlukom

Službenik za zaštitu podataka dužan je dati pisani odgovor ispitaniku u roku od mjesec dana od dana primitka zahtjeva, ili ga pisanim putem obavijestiti da će mu se, zbog složenosti zahtjeva, pisani odgovor dostaviti u roku od dva mjeseca.
Ako u zahtjevu nije moguće utvrditi identitet ispitanika, Službenik za zaštitu podataka može zatražiti dodatne dokaze (ovisno o kanalima koji se koriste za prikaz ili slanje kopije važećeg identifikacijskog dokumenta). U tom slučaju, vrijeme za odgovor počinje teći od trenutka primitka dopunske identifikacijske dokumentacije.

6.7. Naknadna provjera

Praćenje rizika neusklađenosti s propisima o zaštiti osobnih podataka sastoji se – osim definicijom, planiranjem obrada, od odgovarajućih mjera kako bi se uskladilo sa zakonom i pravima ispitanika – naknadnim provjerama adekvatnosti, učinkovite primjene procesa, internih procedura i predložene organizacijske prilagodbe i, općenito, nadziranjem poštovanja vanjskog i unutarnjeg zakonodavstva koje provode korporacijske cjeline.

U ovom kontekstu:
- poslovne funkcije i funkcije podrške, uz pomoć relevantnih kontrolnih funkcija sektora, u skladu s kontrolnim ciljevima koje je utvrdio Službenik za zaštitu podataka te Praćenje usklađenosti, utvrđuju kontrole prve razine te ih dostavljaju Službeniku za zaštitu podataka koji procjenjuje njihovu stvarnu prikladnost za postizanje kontrolnih ciljeva i, po potrebi, zahtijevaju njihovo jačanje
- Službenik za zaštitu podataka, uz podršku Praćenja usklađenosti, utvrđuje kontrole druge razine koje se odnose na zaštitu podataka, utvrđujući ciljeve, učestalost i provedbena pravila
- Unutarnja revizija samostalno određuje kontrole treće razine.

U skladu s definicijom kontrole privatnosti, poslovne funkcije i funkcije podrške te Službenik za zaštitu podataka provode kontrole prve i druge razine te ih dokumentiraju putem izvješća koja izrađuju na posebnom obrascu.

6.8. Širenje kulture zaštite osobnih podataka

Službenik za zaštitu podataka uz potporu Ljudskih resursa i organizacije:
- na godišnjoj razini utvrđuje i ažurira plan edukacije zaposlenika u vezi sa zaštitom osobnih podataka

- priprema i provjerava materijale za edukacije, usmjeravajući aktivnosti potrebne za isporuku edukativnih materijala
- prati sudjelovanje na edukacijama i ishode edukacija.

Godišnjim se planom određuju sudionici edukacija za svaku poslovnu funkciju ili za određene grupe zaposlenika te se utvrđuju oblici edukacije.
Osim uobičajene edukacije, Službenik za zaštitu podataka, uz pomoć Ljudskih resursa i organizacije, organizira i sudjeluje u posebnim inicijativama u svrhu širenja kulture rizika u odnosu na zaštitu osobnih podataka te širenju potrebne razine svijesti pristupa riziku, što obuhvaća naročito:

- uvodnu obuku za poslovne cjeline i radionice za najviše rukovodstvo
- podizanje svijesti poslovnih funkcija i funkcija podrške o posebnim aspektima rizika

6.9. Odnosi s regulatornim tijelima

6.9.1. Odnosi s nadzornim tijelom

Službenik za zaštitu podataka surađuje s nadzornim tijelom za zaštitu podataka, a osobito:

- upravlja odnosima s AZOP-om u vezi s pitanjima usklađenosti ili pitanjima o primjeni propisa, koordinirajući aktivnosti potrebne za dobivanje odgovora, uz potporu Praćenja usklađenosti
- upravlja žalbama koje klijenti podnose AZOP-u te dostavlja odgovarajuće odgovore AZOP-u i ispitaniku

6.9.2. Zahtjevi regulatornih tijela iz treće zemlje

Poslovne cjeline koje primaju zahtjeve za podacima od upravnih ili zakonodavnih tijela treće zemlje, odnosno izvan Europske unije, na temelju sudskih odluka ili upravnih naloga koje izdaju vlasti te treće zemlje, prosljeđuju zahtjev Službeniku za zaštitu podataka koji procjenjuje postoji li:

- međunarodni sporazum (npr. uzajamna pravna pomoć ili slični sporazumi između treće zemlje i Europske unije ili matične države voditelja obrade) ili
- javni interes priznat zakonom države u kojoj voditelj obrade ima poslovni nastan koji zakonom dopušta takav prijenos osobnih podataka.

Ako je ispunjen jedan od navedenih uvjeta, Službenik za zaštitu podataka, uz savjet Pravnih poslova, odobrava prijenos te o tome obavještava nadležno regulatorno tijelo treće zemlje.

7. UPRAVLJANJE GRUPOM

Članice Grupe koje su osnovane u Europskoj uniji obvezne su provoditi ova Politika, prilagođavajući ih situaciji u vlastitom društvu te, u slučaju međunarodnih kompanija, posebnim karakteristikama lokalnih propisa, podnoseći ih tijelu sa strateškom nadzornom funkcijom na odobrenje.

Međunarodne podružnice banaka Grupe smatraju se uredom koji čini dio tih banaka, ali su bez pravne osobnosti te, kao posljedica toga, podružnice ne smiju samostalno provoditi ovu Politiku

budući da će ih izravno usvojiti banke s poslovnim nastanom u Europskoj uniji kojima te podružnice pripadaju.

Praćenje propisa o zaštiti osobnih podataka društava Grupe s poslovnim nastanom u Europskoj uniji obuhvaća dva odvojena modela:

- za posebno utvrđene banke i društva, čije poslovanje pokazuje visok stupanj integracije s matičnim društvom, centralizacija aktivnosti praćenja u matičnome društvu (tzv. centralizirani upravljački model)
- za druga društva s poslovnim nastanom izvan Europske unije, za koje postoji zakonska obveza ili su posebno utvrđena s obzirom na aktivnosti koje obavljaju, imenovanje lokalnoga Službenika za zaštitu podataka (tzv. model savjetovanja, koordinacije i kontrole)

Ovo ne utječe na opću ulogu savjetovanja, koordinacije i kontrole koju provodi Službenik za zaštitu podataka s obzirom na zaštitu privatnosti na temelju Smjernica o usklađenosti Grupe prema društvima koje ne potpadaju pod centralizirani upravljački model i koja imaju poslovni nastan izvan Europske unije.

7.1. Centralizirani upravljački model

Aktivnosti zaštite osobnih podataka koje se moraju provoditi u skladu s ovom Politikom provodi Službenik za zaštitu podataka te druge strukture matičnoga društva, kao i službe Grupe Intese Sanpaolo u skladu sa svojim nadležnostima.

Međunarodne podružnice društava s poslovnim nastanom na području Europske unije obvezne su utvrditi osobu za kontakt koja je nadležna za pomoć Službeniku za zaštitu podataka matičnoga društva pri provođenju njegovih aktivnosti, pravovremeno ga izvješćujući o svim relevantnim događajima i situacijama koje su zakonom propisane kao bitne za zaštitu osobnih podataka.

Takva osoba za kontakt izvješćuje Službenika za zaštitu podataka matičnoga društva.

7.2. Model savjetovanja, koordinacije i kontrole

Obveze članica Grupe s poslovnim nastanom u Europskoj uniji, koje primjenjuju model savjetovanja, koordinacije i kontrole:

- provedba ove Politike, uz dogovor sa Službenikom za zaštitu podataka matičnoga društva Banke o eventualnim usklađenjima njihovom korporativnom i zakonskom kontekstu
- provedba operativnih procesa koje definira matično društvo, u suradnji i uz pomoć Službenika za zaštitu podataka te moguća prilagodba specifičnim poslovnim situacijama
- davanje potrebnih informacija organizacijskim strukturama matičnoga društva o zaštiti osobnih podataka te pravovremenih informacija u slučaju značajnih događaja

Službenik za zaštitu podataka matičnoga društva:

- pruža stručnu pomoć i podršku u području zaštite osobnih podataka
- na zahtjev, pruža podršku lokalnim strukturama u komunikaciji s nadležnim tijelima.

Društva Grupe s poslovnim nastanom u Europskoj uniji koja imaju kontrolni udjel, izravno ili neizravno, moraju uspostaviti najprikladniji organizacijski model za podružnice izvan Europske unije u skladu s uputama matičnoga društva. Također su odgovorna za dostavu Politike matičnoga društva podružnicama te za provjeru njihove ispravne primjene.