

Praćenje usklađenosti

POLITIKA ZAŠTITE OSOBNIH PODATAKA

SADRŽAJ

□	UVOD	4
1	PRAVNI OKVIR	4
2	OPĆA NAČELA	6
3	ULOGE I ODGOVORNOSTI	8
3.1	Korporativna tijela	8
3.2	Uprava Društva	8
3.3	Nadzorni odbor	8
3.4	Odbor za rizike	8
3.5	Službenik za zaštitu podataka	9
3.6	Glavne uključene korporativne funkcije	10
3.6.1	Praćenje usklađenosti	10
3.6.2	Upravljanje rizicima	11
3.6.3	Unutarnja revizija	11
3.6.4	Pravni poslovi	11
3.6.5	Organizacija	12
3.6.6	Poslovne funkcije i funkcije podrške	12
3.6.7	Centralna nabava	13
3.6.8	Ljudski resursi i Organizacija	13
3.6.9	Informacijska i komunikacijska tehnologija	13
3.6.10	Korporativna sigurnost	14
4	MAKRO-PROCESI ZAŠTITE OSOBNIH PODATAKA	15
4.1	Definiranje Politike i metodologije zaštite osobnih podataka	15
4.2	Procjena rizika i okvir sklonosti riziku (RAF)	15
4.3	Planiranje aktivnosti	16
4.4	Regulatorna usklađenost	16
4.5	Identifikacija obrade, metodologija obrade i sigurnosnih mjera (Privacy by Design - Privacy by Default)	16
4.5.1	Utvrđivanje zakonitosti obrade	17
4.5.2	Upravljanje odnosima s trećim stranama i prijenos podataka izvan EU-a	18
4.5.3	Procjena učinka na zaštitu podataka	19
4.5.4	Obrada pomoću sustava umjetne inteligencije (AI)	20
4.6	Upravljanje evidencijom o aktivnostima obrade osobnih podataka	20
4.7	Brisanje podataka	21
4.8	Pravo pristupa podacima	21

4.9	Plan postupanja u slučaju neusklađenosti	22
4.10	Informiranje ispitanika te pribavljanje privole	23
4.11	Upravljanje pravima ispitanika	23
4.12	Aktivnosti nadzora i provjere usklađenosti (Assurance)	24
4.12.1	Interakcije s ostalim kontrolnim funkcijama	24
4.12.2	Proces praćenja	25
4.13	Širenje kulture privatnosti	25
4.14	Odnos s nadzornim tijelima	26
4.14.1	Odnosi s nadzornim tijelima	26
4.14.2	Zahtjevi nadzornih tijela iz treće zemlje	26
4.15	Informacijski tokovi prema korporativnim tijelima	26
5	SMJERNICE I KOORDINACIJA PBZ GRUPE	27
6	DEFINICIJE	27

• UVOD

Ova Politika definira model za upravljanje rizikom neusklađenosti u vezi sa zaštitom osobnih podataka društva PBZ Card d.o.o. (u daljnjem tekstu: Društvo ili PBZC), koje je član PBZ Grupe, pri čemu je PBZ d.d. matično društvo PBZ Grupe (u daljnjem tekstu: Matično društvo), te utvrđuje opća načela i specificira uloge i odgovornosti uključenih tijela i struktura Društva, makro-procese usmjerene na praćenje i upravljanje rizicima te model usmjeravanja i koordinacije između PBZC-a i PBZ Grupe.

1 PRAVNI OKVIR

Europsko zakonodavstvo u području zaštite privatnosti obuhvaća Uredbu (EU) 2016/679 (u daljnjem tekstu: Opća uredba o zaštiti podataka ili GDPR ili Uredba) Europskog parlamenta i Vijeća, donesenu 27. travnja 2016., koja se primjenjuje od 25. svibnja 2018. te uređuje zaštitu osobnih podataka fizičkih osoba i slobodno kretanje takvih podataka unutar Europske unije.

GDPR uređuje obradu osobnih podataka od strane voditelja obrade, što u kontekstu PBZC-a i PBZ Grupe znači pojedinačna društva koja obrađuju osobne podatke, te izvršitelja obrade, koji su u pravilu treće strane izvan PBZC-a i koji obrađuju osobne podatke u ime voditelja obrade.

GDPR se primjenjuje na svu obradu osobnih podataka od strane voditelja ili izvršitelja obrade osnovanih u Europskoj uniji, bez obzira na to provodi li se obrada unutar EU ili na drugi način. Uredba se također primjenjuje na svu obradu osobnih podataka od strane voditelja, ili izvršitelja obrade koji nisu osnovani u Europskoj uniji, a koji obrađuju osobne podatke subjekata koji se nalaze u EU.

GDPR uspostavlja strukturirani niz obveza, od kojih su glavne:

- usvajanje načela privatnosti po dizajnu, tj. zaštite podataka od faze dizajna nadalje, te načela privatnosti po defaultu, tj. zaštita podataka prema zadanim postavkama, kako bi se jamčio nadzor rizika od nepoštivanja zakonodavstva o zaštiti podataka, kako u fazama stvaranja ili značajnih promjena obrade osobnih podataka, tako i tijekom same obrade, usvajanjem kao zadane postavke odgovarajućih tehničkih i organizacijskih mjera za osiguranje odgovarajuće razine sigurnosti;
- provođenje procjene učinka na zaštitu podataka (DPIA), tj. procjene utjecaja na zaštitu podataka prije jedne ili više aktivnosti obrade koje mogu predstavljati visok rizik za prava i slobode fizičkih osoba;
- imenovanje službenika za zaštitu podataka, koji je zadužen za zaštitu osobnih podataka, kada je to potrebno u vezi s obradom informacija u velikom opsegu, kao i osoba ovlaštenih za provedbu obrade te izvršitelja obrade
- utvrđivanje zajedničkih voditelja obrade te formaliziranje relevantnih sporazuma;
- izradu i ažuriranje, na kontinuiranoj osnovi, evidencije o obradi aktivnosti;
- definiranje i održavanje kataloga kontrola;
- obavijest o povredi osobnih podataka AZOP-u i komunikaciji s ispitanicima
- primjena mjera za osiguravanje učinkovite provedbe prava ispitanika koja su definirana Uredbom;
- organiziranje edukacijskih aktivnosti i širenje kulture privatnosti.

Svako kršenje odredbi GDPR-a podložno je 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 korisnik.

GDPR je također predvidio osnivanje Europskog odbora za zaštitu podataka ("EDPB", eng: European Data Protection Board), koji se sastoji od predstavnika nacionalnih nadzornih tijela za zaštitu osobnih podataka država članica Europske unije, EDPB ima ovlast pružiti opće smjernice za pojašnjenje odredbi europskog zakonodavstva o zaštiti podataka, kako bi adresatima tih odredbi pružila jedinstvena interpretacija njihovih prava i obveza. Osim toga, EDPB može donositi obvezujuće odluke u skladu s GDPR-om upućene nacionalnim nadzornim tijelima, s ciljem osiguravanja ujednačene primjene propisa.

Najznačajnije aktivnosti EDPB-a uključuju:

- Odobrenje 1/2018 kojom se potvrđuju smjernice prethodno navedene u WP29¹;
- Smjernice 3/2018 o teritorijalnom opsegu GDPR-a (članak 3);
- Smjernice 2/2019 o obradi osobnih podataka prema članku 6(1)(b) GDPR-a u kontekstu pružanja online usluga ispitanicima;
- Smjernice 3/2019 o obradi osobnih podataka posredstvom video nadzora;
- Smjernice 4/2019 o članku 25(Data Protection by Design i by Default);
- Smjernice 05/2020 o privoli sukladno GDPR-u
- Smjernice 06/2020 o međusobnom djelovanju Druge direktive o Plaćanju i GDPR-a;
- Smjernice 07/2020 o konceptu voditelja obrade i izvršitelja obrade osobnih podataka po GDPR-u;
- Preporuke 01/2020 o mjerama koje zamjenjuju prijenosna sredstva s ciljem osiguranja usklađenosti na razini EU u odnosu na zaštitu osobnih podataka;
- Smjernice 10/2020 o ograničenjima prema članku 23 GDPR-a;
- Smjernice 01/2021 o primjerima prijave povrede osobnih podataka;
- Smjernice 05/2021 o međusobnom odnosu između članka 3. i odredbi o međugraničnom prijenosu sukladno Poglavlju V GDPR-a;
- Smjernice 01/2022 o pravima ispitanika - Pravo na pristup;
- Smjernice 03/2022 o obmanjujućim obrascima dizajna na sučeljima društvenih mreža: kako ih prepoznati i izbjeći;
- Smjernice 07/2022 o certificiranju kao sredstvu za prijenos;
- Smjernice 09/2022 o obavještanju o povredama osobnih podataka prema GDPR-u;
- Smjernice 08/2022 o identifikaciji voditelja obrade ili vodećeg nadzornog tijela izvršitelja obrade;
- Smjernice 05/2022 o upotrebi tehnologije prepoznavanja lica u području izvršavanja zakonodavstva;
- Smjernice 2/2023 o tehničkom području primjene članka 5. stavka 3. Direktive o e-privatnosti;
- Mišljenje 28/2024 o određenim aspektima zaštite podataka vezanim uz obradu osobnih podataka u kontekstu AI modela;
- Smjernice 01/2024 o obradi osobnih podataka na temelju članka 6(1)(f) GDPR-a

Dodatno, u pogledu aspekata povezanih s korištenjem sustava umjetne inteligencije u kontekstu obrade podataka u bankarstvu, upućuje se na Uredbu (EU) 2024/1689 o umjetnoj inteligenciji („AI Act“).

¹ Radna skupina prema članku 29 (WP29) bila je neovisna europska radna skupina koja se do 25. svibnja 2018. (datum stupanja GDPR-a na snagu) bavila pitanjima zaštite pojedinaca i osobnih podataka.

U pogledu nacionalnog zakonodavstva i dalje se primjenjuju odredbe Zakona o provedbi Opće uredbe o zaštiti podataka (NN 42/2018).

U odnosu na zemlje izvan Europske unije, gdje djeluju članice PBZ Grupe, na snazi su propisi o zaštiti privatnosti.

2 OPĆA NAČELA

Društvo priznaje stratešku važnost nadzora nad rizicima neusklađenosti, koji uključuje sustav upravljanja za zaštitu osobnih podataka fizičkih osoba s kojima Društvo komunicira. Pravo na zaštitu osobnih podataka, odnosno pravo na privatnost, temeljno je pravo ljudi, izravno povezano s očuvanjem ljudskog dostojanstva, koje se također utvrđuje u Povelji Europske unije o temeljnim pravima.

Poštivanje prava i sloboda osoba predstavlja identifikacijski i vrijedan element za Društvo. Kako je navedeno u načelima vlastitog Etičkog kodeksa, radi jamčenja zaštite sigurnosti klijenata, njihove imovine i informacija, Društvo, u skladu sa zakonima u svakom trenutku, obvezuje se:

- 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;
- Dosljedno poštuju kriterije transparentnosti u informiranju klijenata o njihovim pravima na privatnost i načinu na koji se obrađuju njihovi osobni podaci.

U tu svrhu Društvo primjenjuje model kojim se osigurava da se osobni podaci:

- obrađuju zakonito, pošteno i transparentno u odnosu na ispitanika
- prikupljaju samo za specifične, eksplicitne i legitimne svrhe i da se dalje ne obrađuju na način koji nije u skladu s tim svrhama (ograničenje svrhe);
- adekvatni, relevantni i ograničeni na ono što je potrebno za svrhu obrade (minimizacija podataka);
- točni, i kad je to potrebno, ažurni uz ulaganje svih napora 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).

Usvojeni model zaštite osobnih podataka unutar je okvira Pravilnika o integriranom sustavu unutarnje kontrole, pri čemu se zaštita podataka provodi kroz sve korporativne funkcije koje rade zajedno;

- Korporativna tijela odgovorna su za osiguravanje adekvatnog nadzora nad rizicima neusklađenosti;
- Službenik za zaštitu podataka, koji u organizacijskom smislu spada pod funkciju usklađenosti, prati rizik neusklađenosti putem pristupa temeljenog na riziku, djelujući neovisno;

- poslovne i funkcije podrške provode obradu, utvrđujući unaprijed, uz pomoć službenika za zaštitu podataka, svrhe i procedure, usklađujući se s korporativnim procesima i procedurama te procjenjujući njihovu primjenu, na temelju odgovarajućih kontrola prve razine, s ciljem potpunog i potpunog usklađivanja s važećim pravilima i standardima ponašanja.
- Funkcija interne revizije PBZ d.d. (kao dobavljač outsourcing aktivnosti za PBZC), kao dio vlastitih aktivnosti za praćenje treće razine sustava unutarnje kontrole, procjenjuje adekvatnost i učinkovitost modela upravljanja rizicima usklađenosti.

Svaka organizacijska struktura odgovorna je za obradu podataka, a svaki zaposlenik, kao i vanjski suradnici Društva, bez obzira na njihov ugovorni odnos, te općenito strane koje obavljaju obradu za koju ih je Društvo ovlastilo u svojstvu ovlaštenih osoba za obradu, moraju se pridržavati uputa koje Društvo daje tijekom aktivnosti, poštivanje obveza povjerljivosti i sigurnosti 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, sigurnosne mjere za pristup računalnim aplikacijama (kontrola pristupa) dizajnirane su i provedene tako da minimiziraju pristup podacima, ograničavajući ga samo na osobe čije su aktivnosti strogo funkcionalne za tu svrhu. 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.

Društvo posebnu pažnju posvećuje korištenju Big Data, što znači velike količine, brze i raznovrsne IT resurse koji podrazumijevaju inovativne oblike analize i obrade podataka, osiguravajući poštivanje prava i sloboda ispitanika te usvajanjem potrebnih mjera za zaštitu i, u skladu s sa svrhom obrade, anonimizacije.

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

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

Ova Politika podložna je reviziji u slučaju značajnih pravnih promjena, u skladu s organizacijskim i operativnim promjenama u modelu nadzora rizika neusklađenosti u vezi s zaštitom osobnih podataka.

3 ULOGE I ODGOVORNOSTI

3.1 *Korporativna tijela*

Na razini Matičnog društva, organizacijske jedinice Matičnog društva odgovorne su, svaka prema vlastitim kompetencijama i ovlastima, za osiguranje adekvatnog upravljanja rizikom usklađenosti kojem je PBZ Grupa izložena ili bi mogla biti. Posebno, funkcija praćenja usklađenosti Matičnog društva odgovorna je za upravljanje rizicima neusklađenosti u vezi s zaštitom osobnih podataka te u tu svrhu odobrava i pregledava Politiku o zaštiti osobnih podataka te nadzire pravilnu primjenu politika i propisa Grupe o zaštiti osobnih podataka. Također, funkcija praćenja usklađenosti Matičnog društva redovito prima informacije od Društva o važnim pitanjima vezanim uz zaštitu podataka i, u okviru redovite komunikacije, pomaže Društvu u provedbi zaštite osobnih podataka, ako je potrebno.

Na razini Društva, i u skladu s načelom koje je uspostavilo Matično društvo, ova Politika u nastavku definira uloge i odgovornosti korporativnih tijela Društva.

3.2 *Uprava*

S obzirom na nadzor rizika neusklađenosti u vezi sa zaštitom osobnih podataka, Uprava Društva:

- odobrava model upravljanja rizikom neusklađenosti u vezi s zaštitom osobnih podataka (relevantne osobe, 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, poput stručnog znanja o zakonodavstvu o zaštiti osobnih podataka i organizacijskoj strukturi Društva.
- prima informacije, najmanje jednom godišnje, od Službenika za zaštitu podataka o posebno važnim pitanjima vezanim uz zaštitu podataka;
- odmah se obavještava u slučaju ozbiljnih problema vezanih uz poslovnu aktivnost koja proizlazi iz povrede povjerljivosti, o dostupnosti ili integritetu osobnih podataka;
- pregledava godišnja izvješća pripremljena od strane kontrolnih funkcija Društva.

3.3 *Nadzorni odbor*

U pogledu praćenja rizika neusklađenosti u vezi sa zaštitom 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 u poslovnoj aktivnosti koji proizlaze iz kršenja povjerljivosti, dostupnosti ili integriteta osobnih podataka, Nadzorni odbor se obavještava bez odgađanja, koji će pregledati godišnja izvješća koja sastavljaju kontrolne funkcije Društva.

3.4 *Odbor za rizike*

Odbor za rizike podupire Nadzornom odboru kako bi se osigurala najbolja kontrola rizika neusklađenosti u pogledu zaštite osobnih podataka; U tom kontekstu, zadaci spomenuti u odlomku 3.2. podnose na znanje Odboru za upravljanje rizicima.

3.5 Službenik za zaštitu podataka

Službenik za zaštitu podataka (u daljnjem tekstu: DPO) ima zadatak pružanja savjetovanja i praćenja poštivanja GDPR-a od strane Društva, procjenjujući rizike svake obrade u pogledu njezine prirode, opsega primjene, konteksta i svrhe, te definirajući postupke praćenja i povezane kontrole.

Uprava Društva imenuje Službenika za zaštitu podataka koji:

- mora ispunjavati uvjete primjerenosti propisane zakonom te posjedovati neovisnost, autoritet i profesionalnost, uključujući stručno znanje o zakonodavstvu i praksi zaštite osobnih podataka te organizacijskoj strukturi Društva;
- je neovisan u obavljanju svojih dužnosti;
- ne smije biti udaljen s položaja niti kažnjen zbog obavljanja svojih dužnosti;
- ima primjerene ovlasti raspolaganja sredstvima, prepoznate prilikom postavljanja na funkciju;
- odgovoran je direktno korporativnim tijelima Društva.

Službenik za zaštitu podataka, samo u vezi s regulatornim područjima iz svoje nadležnosti, ima pristup svim aktivnostima Društva, kao i svim informacijama važnim za obavljanje svojih dužnosti putem izravnog kontakta sa zaposlenicima.

U tu svrhu:

- ostale korporativne strukture Društva dužne su pravovremeno i u potpunosti obavijestiti Službenika za zaštitu podataka o svakom značajnom događaju, radi nadzora rizika od neusklađenosti;
- Službenik za zaštitu podataka ima pravo tražiti i pravovremeno primiti od drugih korporativnih struktura Društva sve dodatne informacije relevantne za obavljanje svojih dužnosti.

S obzirom na zakonodavstvo vezano uz zaštitu osobnih podataka, Službenik za zaštitu podataka primjenjuje makro-procese definirane Politikom usklađenosti i metode procjene rizika neusklađenosti zajedno s Praćenjem usklađenosti Matičnog društva.

Posebno, Službenik za zaštitu podataka:

- provodi Politiku i interne akte iz područja zaštite osobnih podataka koje je usvojila Uprava Društva;
- osigurava provedbu modela nadzora zaštite osobnih podataka i provodi inicijative i mjere potrebne za osiguranje njegove potpunosti, adekvatnosti, funkcionalnosti i pouzdanosti na kontinuiranoj osnovi;
- usvaja potrebne korektivne mjere ili odgovarajuće prilagodbe u slučaju da se pojave nedostaci ili slabosti u radu modela kontrole;
- pruža podršku poslovnim funkcijama i funkcijama podrške dajući mišljenje u slučaju povrede povjerljivosti, dostupnosti ili integriteta osobnih podataka te pruža informacije Upravi društva u slučaju ozbiljnih problema s poslovnim aktivnostima koje iz njih proizlaze;
- pruža podršku poslovnim funkcijama u Procjeni učinka na zaštitu podataka (DPIA) davanjem svog mišljenja i praćenjem njezine provedbe
- pruža podršku poslovnim funkcijama i funkcijama podrške u procjeni događaja koji se mogu smatrati povredom osobnih podataka (Data Breach), te potrebi obavješćavanja AZOP-a i/ili ispitanika;

- skreće pozornost Upravi Društva na pitanja vezana uz zaštitu osobnih podataka koja se smatraju osobito važnima te joj dostavlja informacije najmanje jednom godišnje;
- informira zaposlenike i podiže njihovu svjesnost o obvezama koje proizlaze iz Uredbe i drugih pravila vezanih uz zaštitu osobnih podataka;
- surađuje s AZOP-om i djeluje kao kontakt osoba tog tijela za svako pitanje povezano s obradom, uključujući prethodne savjetovanje nakon Procjene učinka na zaštitu podataka (DPIA);
- pruža podršku operativnim i poslovnim funkcijama u vezi sa svakom aktivnošću povezanom s obradom osobnih podataka;
- provodi test ravnoteže legitimnog interesa u svrhu utvrđivanja mogućnosti primjene legitimnog interesa kao pravne osnove za obradu;
- upravlja povratnim informacijama AZOP-u i ispitanicima nakon žalbi, izvješća ili pritužbi podnesenih nadležnom tijelu i obrađuje zahtjeve za ostvarivanje prava ispitanika; procjenjuje kontrole prve razine koje predlažu poslovne ili operativne funkcije te u suradnji s Praćenjem usklađenosti Matičnog društva definira kontrole druge razine vezane uz zaštitu podataka, utvrđuje njihove ciljeve, učestalost i način izvršenja;
- obavlja kontrolu druge razine zaštite osobnih podataka;
- uspostavlja i vodi evidenciju aktivnosti obrade u suradnji s poslovnim funkcijama i funkcijama podrške;
- provjerava, najmanje jednom godišnje, usklađenost ove politike s relevantnim zakonodavstvom i internim propisima te predlaže njihovo ažuriranje uz podršku Ljudskih resursa i Organizacije Matičnog Društva
- predlaže organizacijske i proceduralne promjene s ciljem osiguravanja odgovarajuće rizika neusklađenosti

Službenik za zaštitu podataka izravno izvještava korporativna tijela te ima podršku tima zaduženog za usklađenost s GDPR-om.

Neovisnost Službenika za zaštitu podataka očituje se u tome što se on ne smije biti razriješen s dužnosti niti kažnjen zbog izvršavanja svojih zadaća, pri čemu se u vrijeme njegovog imenovanja utvrđuje prikladan proračun troškova te njegovi zadaci kao dio ove Politike i Procedura.

3.6 Glavne uključene korporativne funkcije

3.6.1 Praćenje usklađenosti

Na temelju Smjernica za usklađenost, Praćenje usklađenosti:

- definira, u suradnji sa Službenikom za zaštitu podataka, metode procjene rizika od neusklađenosti i odgovarajuće postupke za njegovo ublažavanje;
- pruža podršku Službenika za zaštitu podataka pri utvrđivanju kontrola druge razine;
- izražava, na temelju periodičnih izvješća i dodatnih informacija koje pružaju Službenik za zaštitu podataka i ostale kontrolne funkcije Društva te na temelju izravno provedenih provjera, neovisnu procjenu rizika neusklađenosti sa zakonodavstvom o zaštiti osobnih podataka i adekvatnosti uspostavljenih mjera za njegovo ublažavanje te, ako se ukaže potreba, zahtijeva od Službenika za zaštitu podataka poduzimanje odgovarajućih inicijativa za njihovo jačanje.

- 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.

3.6.2 Upravljanje rizicima

U vezi s upravljanjem rizikom neusklađenosti u području zaštite osobnih podataka, funkcija Upravljanja rizicima Matičnog društva surađuje sa Službenikom za usklađenost i Službenikom za zaštitu podataka radi definiranja metoda procjene rizika neusklađenosti, potičući sinergiju s alatima i metodama za upravljanje operativnim i reputacijskim rizicima.

3.6.3 Unutarnja revizija

Unutarnja revizija kao pružatelj centralizirane aktivnosti, u okviru svojih aktivnosti praćenja cjelokupnog sustava internih kontrola, periodično procjenjuje potpunost, primjerenost, funkcionalnost (u smislu učinkovitosti i djelotvornosti) i pouzdanost modela upravljanja rizikom neusklađenosti Društva te surađuje sa Službenikom za usklađenost i ostalim funkcijama nadležnima za kontrolu tog rizika, kako bi provjerila stvarnu primjenu internih i eksternih propisa od strane Društva te upravljala svim nedostacima utvrđenima tijekom revizorskih aktivnosti.

Nakon provedenih kontrola i procjena, unutarnja revizija prijavljuje sve nepravilnosti vezane uz obradu osobnih podataka nadležnim korporativnim strukturama i Službeniku za zaštitu podataka te o tome izvješćuje Upravu Društva.

3.6.4 Pravni poslovi

Pravni poslovi u vezi sa zakonodavstvom o zaštiti osobnih podataka:

- pruža podršku Službeniku za zaštitu podataka u kontinuiranom utvrđivanju primjenjivih zakonskih odredbi, praćenju njihovog razvoja, uključujući sudsku praksu, te njihovu tumačenju
- podržavaju službenika za zaštitu podataka u testu balansiranja interesa radi utvrđivanja pravne osnove u legitimnom interesu;
- pruža podršku Službenika za zaštitu podataka u utvrđivanju mjera koje doprinose osiguravanju zakonitosti obrade u procesu procjene utjecaja učinka na zaštitu podataka (DPIA);
- utvrđuje, uz podršku Službenika za zaštitu podataka, uvjete za pohranu osobnih podataka;
- pruža podršku, u pogledu pravnih aspekata, Službeniku za zaštitu podataka u izradi ugovornih klauzula, obrazaca, komunikacije s ispitanicima te u ispitivanju značajnih slučajeva utvrđenih nepravilnosti

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

3.6.5 Organizacija

U vezi s upravljanjem rizikom neusklađenosti u području zaštite osobnih podataka, Organizacija Matičnog društva, u dogovoru sa Službenikom za zaštitu podataka:

- definira organizacijska rješenja u skladu s ciljevima i smjernicama u području zaštite osobnih podataka. Osobito nadzire analizu i usvajanje procesa organizacijskih promjena i razvoja, koji također proizlaze iz nužnih 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 ove Politike, utvrđujući potrebne uloge i odgovornosti.

3.6.6 Poslovne funkcije i funkcije podrške

Poslovne funkcije i funkcije podrške Društva odgovorne su za proces upravljanja rizicima neusklađenosti vezanim uz zaštitu osobnih podataka.

Pridržavaju se korporativnih procesa i procedura, provjeravajući njihovu primjenu odgovarajućim kontrolama prve razine, s ciljem osiguravanja ispravnog obavljanja aktivnosti te potpunog i sveobuhvatnog poštivanja primjenjivih pravila i standarda ponašanja. Kontrole prve razine koje se odnose na zaštitu osobnih podataka, a identificiraju ih poslovne funkcije i funkcije podrške, pregledava Službenik za zaštitu podataka, koji procjenjuje njihovu stvarnu sposobnost postizanja kontrolnih ciljeva te, gdje je to potrebno, traži njihovo jačanje. U slučajevima kada poslovne funkcije i funkcije podrške identificiraju ključne probleme, bilo izravno ili prema uputama odgovarajućih kontrolnih funkcija Društva na razinama druge i treće razine, poduzimaju potrebne mjere za rješavanje tih problema.

Poslovne funkcije i funkcije podrške:

- aktivno sudjeluju u provedbi obveza propisanih zakonodavstvom u području zaštite osobnih podataka, a koje su uređene posebnim smjernicama, procesima i internim politikama 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 učinka na zaštitu podataka (DPIA);
- 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:
 - o finaliziraju, uz pomoć Pravnih poslova i Službenika za zaštitu podataka, ugovor o obradi osobnih podataka između voditelja obrade i izvršitelja obrade te ugovor ili drugi pravni akt u slučaju imenovanja zajedničkih voditelja obrade;

- formaliziraju ugovorne uvjete potrebne za prijenos osobnih podataka izvan teritorija Europske unije, koje utvrde Službenik za zaštitu podataka i Pravni poslovi;
- pomažu kako bi se programi za obuku 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.

3.6.7 Centralna nabava

U vezi s upravljanjem rizikom neusklađenosti u području zaštite osobnih podataka Centralna nabava, u okviru centralizirane aktivnosti koju pruža PBZ d.d. kao Matično društvo:

- 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;
- formalizira ugovorne uvjete koji su potrebni za prijenos osobnih podataka izvan teritorija Europske unije koje utvrde Službenik za zaštitu podataka i Pravni poslovi.

3.6.8 Ljudski resursi i organizacija

U vezi s upravljanjem rizikom neusklađenosti u području zaštite osobnih podataka Ljudski resursi i Organizacija, u okviru centralizirane aktivnosti koju pruža PBZ d.d., kao Matično društvo:

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

U vezi s upravljanjem rizika neusklađenosti u području zaštite osobnih podataka, Ljudski resursi i Organizacija, ima aktivnu ulogu pri provođenju disciplinskih mjera prema zaposlenicima koji su prijavljeni za nepravilnosti pri radu, provođenjem sljedećih aktivnosti:

- procjenjuje i predlaže disciplinske mjere prema zaposlenicima prijavljenima zbog nepravilnosti u radu u odnosu na obveze iz propisa o zaštiti osobnih podataka;
- procjenjuju primjenjivost zaštitnih mjera propisanih kolektivnim ugovorom za zaposlenike protiv kojih se vode kazneni, građanski ili upravni postupci zbog navodnih povreda propisa o zaštiti osobnih podataka

3.6.9 Informacijska i komunikacijska tehnologija

U vezi s upravljanjem rizikom neusklađenosti u području zaštite osobnih podataka, Informacijska i komunikacijska tehnologija zadužena je, u okviru centralizirane aktivnosti koju pruža PBZ d.d., kao Matično društvo, zadužena je za:

- provedbu odgovarajućih tehničkih mjera utvrđenih uz podršku Službenika za zaštitu podataka;

- pružanje podrške Službeniku za zaštitu podataka u utvrđivanju područja primjene aplikacija koja mogu imati utjecaj na obradu osobnih podataka;
- uključuje Službenika za zaštitu podataka u slučaju IT intervencija ili razvoja aplikacija ili softvera koji mogu utjecati na obradu osobnih podataka, radi prethodne procjene mogućih utjecaja na privatnost;
- izvršenje mitigacijskih mjera koje je prijavio Službenik za zaštitu podataka.

3.6.10 Korporativna sigurnost

U vezi s upravljanjem rizika neusklađenosti u području zaštite osobnih podataka, Korporativna sigurnost, kao dio centralizirane aktivnosti koju pruža PBZ d.d., kao Matično društvo, zadužena je za:

- utvrđivanje, uz podršku Službenika za zaštitu podataka, pravila i mjera za zaštitu podataka, informacija i infrastrukture radi održavanja sigurnosnih uvjeta u skladu s važećim propisima;
- sudjeluje u Procjeni učinka na zaštitu podataka (radi utvrđivanja i definiranja sigurnosnih mjera koje će se primjenjivati na obradu osobnih podataka);
- uključuje Službenika za zaštitu podataka u slučaju sigurnosnih događaja koji se odnose na osobne podatke radi utvrđivanja povreda osobnih podataka, koje je potrebno prijaviti AZOP-u i/ili o kojima će se obavijestiti ispitanici, kao i pripremu mitigacijskih mjera usmjerenih sa ciljem suzbijanja i uklanjanja takvih događaja;
- pruža podršku, za sigurnosne aspekte, poslovnim funkcijama i funkcijama podrške radi utvrđivanja tehničkih i organizacijskih mjera kojima se osigurava razina nadzora primjerena profilu rizika obrade.

4 MAKRO PROCESI ZAŠTITE OSOBNIH PODATAKA

Utvrđeni su sljedeći glavni makro procesi koji opisuju metode praćenja i kontrole rizika neusklađenosti koji se odnose na zaštitu osobnih podataka:

1. definiranje Politike i metodoloških pravila za zaštitu osobnih podataka;
2. procjena rizika i okvir sklonosti riziku (RAF, eng. Risk Appetite Framework);
3. planiranje aktivnosti zaštite osobnih podataka;
4. usklađivanje s važećim propisima;
5. identifikaciju obrade osobnih podataka te definiranje metoda obrade i sigurnosnih mjera (Privacy by Design - Privacy by Default);
6. vođenje evidencijom aktivnosti obrade osobnih podataka;
7. brisanje podataka;
8. pristup podacima;
9. upravljanje događajima neusklađenosti i incidentima;
10. informiranje ispitanika i pribavljanje privola;
11. upravljanje pravima ispitanika;
12. aktivnosti koje osiguravaju da je Društvo usklađeno s relevantnim propisima o zaštiti podataka (eng. Assurance);
13. širenje korporativne kulture adekvatnog upravljanja osobnim podacima;
14. suradnja s nadležnim regulatornim tijelima;
15. periodična razmjena informacija prema korporativnim tijelima.

4.1 Definiranje politike i metodologije zaštite osobnih podataka

Službenik za zaštitu podataka definira Politiku, okvir i metodologiju za praćenje i procjenu rizika neusklađenosti u vezi sa zaštitom osobnih podataka na razini PBZC-a.

Konkretno, Službenik za zaštitu podataka:

- definira i ažurira interne akte, ovu Politiku kao i druge interne akte npr. smjernice, pravila, procesne upute, kataloge kontrola putem stalnog praćenja - uz pomoć Pravnih poslova, s ciljem identifikacije i implementacije promjena primjenjivih propisa koji se odnose na zaštitu osobnih podataka;
- definira i ažurira metodologije upravljanja rizicima u području zaštite osobnih podataka;
- predlaže organizacijske i procesne izmjene s ciljem osiguravanja odgovarajućeg nadzora rizika usklađenosti vezanih uz zaštitu privatnosti.

4.2 Procjena rizika i okvir sklonosti riziku (RAF)

Službenik za zaštitu podataka identificira i procjenjuje rizik neusklađenosti i povezanih ranjivosti barem jednom godišnje. Procjena se provodi na temelju metodologije iz područja upravljanja Glavnog službenika za praćenje usklađenosti ISP-a i Glavnog službenika za upravljanje rizikom ISP-a (eng. *Chief Risk Officer*), a povezani rezultati unose se u Procjenu rizika usklađenosti i Integriranu procjenu rizika te se također uzimaju u obzir unutar RAF okvira.

4.3 Planiranje aktivnosti

Rizici neusklađenosti i povezane ranjivosti identificiraju se i procjenjuju prije planiranih aktivnosti upravljanja koji se podnose, kao dio godišnjih izvještaja, Upravi Društva na odobrenje. Službenik za zaštitu podataka nadgleda godišnje planiranje, uzimajući u obzir aktivnosti koje treba provesti, u smislu prioriteta, ciljeva, vremena i korištenja ljudskih i financijskih resursa.

4.4 Regulatorna usklađenost

Nadzor rizika neusklađenosti provodi se preventivno, prvenstveno kako bi se osiguralo kontinuirano praćenje zakonodavnog okvira i tumače kao smjernice, pravila, procesi i interne procedure.

Regulatorna usklađenost zajamčena je sljedećim aktivnostima:

- kontinuirano identificiranje i tumačenje primjenjivog zakonodavnog okvira, kroz kontinuirano praćenje pravnih izvora i konsolidaciju nedvosmislenog, zajedničkog tumačenja, u slučaju promjene u zakonodavnom okviru.
- procjenu utjecaja primjenjivih propisa na korporativne procese i procedure Društva te posljedične prijedloge organizacijskih i procesnih promjena usmjerenih na osiguranje adekvatnog nadzora nad rizicima neusklađenosti.

Službenik za zaštitu podataka kontinuirano provodi aktivnosti identificiranja vanjskih propisa, uz podršku Pravnih poslova, u svrhu tumačenja. Službenik za zaštitu podataka procjenjuje utjecaj primjenjivih propisa i sukladno tome predlaže smjernice, pravila, procese i procedure za zaštitu osobnih podataka, uz pomoć Ljudskih resursa i organizacije, a za pravne aspekte i Pravnih poslova.

4.5 Identifikacija obrade, definiranje metoda obrade i sigurnosnih mjera (Privacy by Design - Privacy by Default)

Identifikacija i evidentiranje obrada osobnih podataka koje se provode ili se planiraju provoditi predstavljaju aktivnosti koje prethode usvajanju i usklađivanju sa zakonodavstvom vezanim uz zaštitu osobnih podataka.

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

U tu svrhu, poslovne funkcije i funkcije podrške:

- identificiraju pojedinačne obrade, pripadajuće svrhe, ulogu svih uključenih sudionika i kategorije primatelja kojima se podaci prenose ili mogu biti preneseni;
- provjeravaju zakonitost obrade uz podršku Službenika za zaštitu podataka, a po potrebi i Pravnih poslova;
- osiguravaju, uz podršku Službenika za zaštitu podataka, da se prema zadanim postavkama obrađuju samo osobni podaci koji su nužni 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 učinka na zaštitu podataka (Data Protection Impact Assessment /DPIA);
- provjeravaju uključenost trećih strana i traže od Službenika za zaštitu podataka da procijeni ulogu koju treba dodijeliti trećim stranama (voditelj obrade, izvršitelj obrade, zajednički voditelj obrade);
- utvrđuju eventualne potrebe za prijenos podataka izvan EU te zahtijevaju od Službenika za zaštitu podataka utvrđivanje odgovarajućih zaštitnih mjera;
- 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 zaštite za stupanj rizika obrada s posebnim naglaskom na pristup podacima.

Procjene utjecaja i donesene odluke dokumentira i pohranjuje Službenik za zaštitu podataka kako bi osigurao poštovanje načela odgovornosti. Dubina provedenih analiza proporcionalna je razini složenosti i novim aspektima razmatranih slučajeva obrade, kao i primjenjivom zakonodavstvu.

Poslovne funkcije i funkcije podrške identificiraju obradu u slučajevima:

- razvoja novih proizvoda ili usluga ili njihovih bitnih promjena, uključujući potrebne IT intervencije (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, prijenosi ili prodaje)
- primjene Big Data obrade velikih opsega;
- bilo kojem drugom slučaju pokretanja ili izmjene obrade osobnih podataka.

4.5.1 Utvrđivanje zakonitosti obrade

Kako bi se utvrdila zakonitost obrade, poslovne funkcije i funkcije podrške uz pomoć Službenika za zaštitu podataka i prema potrebi Pravnih poslova, identificiraju pravni temelj obrade koji može biti:

- privola;
- izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora;
- zakonska obveza kojoj Društvo podliježe;
- legitimni interes 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 prijevare na štetu Društva);
- da je obrada neophodna za ostvarivanje temeljnog prava ili se obavlja u javnom interesu, uzimajući u obzir moguću štetu koja bi nastala za Društvo 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.

Obrada povezana s automatiziranim procesom donošenja odluka zakonita je ako:

- je nužna za izvršenje ugovora ili u svrhu sklapanja ugovora u kojemu je ispitanik stranka;
- dopuštena je zakonom EU ili države članice koji mora poštivati voditelj obrade, koji također određuje odgovarajuće mjere za zaštitu prava, sloboda i legitimnih interesa ispitanika;
- se temelji 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, spolni život ili spolnu 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 u skladu s važećim zakonima;
- se odnosi na osobne podatke koje je ispitanik učinio javno dostupnima;
- je potrebno utvrditi, ostvarivati ili braniti pravo na sudu;
- je neophodno iz razloga značajnog javnog interesa na temelju prava EU ili država članica;
- je neophodno za potrebe arhiviranja u javnom interesu, za znanstvena ili povijesna istraživanja ili za statističke svrhe na temelju EU 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, te da ispitanik može ostvariti svoja zakonska prava; primjerice u slučaju obrade koja uključuje proces automatiziranog odlučivanja, pravo na ljudsku intervenciju, izražavanje mišljenja, dobivanje objašnjenja donesene odluke ili osporavanje odluke.

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

U pogledu obrade osobnih podataka koje Društvo povjerilo trećim osobama (uključujući dobavljače/treće strane i eventualne poddobavljače (podizvršitelje), 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 ugovora o obradi osobnih podataka, čiji se tekst utvrđuje uz pomoć Pravnih poslova i Službenika za zaštitu podataka.

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

U slučaju uspostavljanja poslovnog odnosa s trećim stranama ili članicama Grupe koje dovodi do zajedničkog utvrđivanja svrha i sredstava obrade osobnih podataka, 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.

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 i svrhom obrade te, kad je potrebno, postoje li privole ispitanika, te utvrđuje uz pomoć Pravnih poslova s tim povezane ugovorne metode i uvjete

4.5.3 Procjena učinka na zaštitu podataka

Ako procjena potencijalnih rizika obrade pokaže 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 učinka na zaštitu podataka – engl. Data Protection Impact Assessment – DPIA, u daljnjem tekstu: DPIA) kako bi se definirale odgovarajuće tehničke i organizacijske sigurnosne mjere.

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

Rezultat Procjene učinka na zaštitu podataka 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 učinka na zaštitu podataka. 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 obustaviti postojeću obradu.

Službenik za zaštitu podataka periodično pregledava sve obrade visokog rizika, provodeći Procjenu učinka na zaštitu podataka s različitom učestalošću, ovisno o vrsti obrade i riziku za prava i slobode ispitanika.

4.5.4 Obrada pomoću sustava umjetne inteligencije (AI)

Prilikom upotrebe sustava umjetne inteligencije (AI), poslovne funkcije i funkcije podrške moraju biti posebno oprezne u pogledu zaštite podataka, s obzirom na to da ti sustavi mogu donijeti značajne koristi, ali također mogu uključivati rizike i ugroziti javne interese i zaštićena prava. Procjene obrada koje uključuju AI sustave moraju se strogo provoditi u skladu s načelima sadržanima u "Smjernicama Grupe za uporabu umjetne inteligencije". Procjene trebaju biti integrirane u standardne, formalno regulirane procese, pri čemu se posebna pažnja mora posvetiti nadzoru pitanja koja su u nadležnosti relevantnih funkcija uključenih u proces.

Kada poslovne funkcije i funkcije podrške koriste AI sustave koji uključuju obradu osobnih podataka, moraju se pridržavati načela GDPR-a u svim fazama obuke i korištenja tih sustava.

Uz podršku Službenika za zaštitu podataka, potrebno je osigurati i dokazati usklađenost s načelima zaštite osobnih podataka, što obuhvaća sljedeće:

- pravni temelj obrade podataka, za sve faze razvoja i konfiguracije AI sustava, kako je navedeno u informaciji o zaštiti osobnih podataka koja je pružena ispitanicima;
- osiguravanje da se u razvoju modela koriste isključivo nužne informacije te, kada je to moguće, provođenje anonimizacije podataka, a ako anonimizacija nije moguća;
- mogućnost konfiguracije u slučajevima gdje se provodi profiliranje ili automatizirano odlučivanje, provjera postojanja zaštitnih mjera propisanih zakonodavstvom, posebno u pogledu transparentnosti i prava ispitanika;
- neekskluzivnost algoritamske odluke - u slučajevima automatiziranih procesa nužno je osigurati ljudsku intervenciju, čime se osigurava da odluke nisu u potpunosti prepuštene algoritmu
- ispravna formalizacija ugovornih odnosa s pružateljima AI rješenja, kako bi se osigurala usklađenost sa zakonodavstvom.

4.6 Upravljanje evidencijom o aktivnostima obrade osobnih podataka

Službenik za zaštitu osobnih podataka uspostavlja evidencije obrade osobnih podataka procjenjujući zahtjeve propisane Uredbom. Obrada osobnih podataka je evidentirana od poslovnih i pomoćnih funkcija u Društvu, a ta evidencija minimalno uključuje informacije propisane Uredbom.

Informacije potrebne za evidentiranje obrada prikupljaju se tijekom procesa „Identifikacija obrade, metodologija obrade i sigurnosnih mjera (Privacy by Design - Privacy by Default)“. Službenik za zaštitu podataka periodično, a minimalno jednom godišnje, provjerava Evidenciju obrade te listu voditelja i izvršitelja obrade.

Službenik za zaštitu podataka osigurava da je Evidencija aktivnosti obrada promptno dostupna na zahtjev nadzornog tijela.

4.7 *Brisanje podataka*

Cilj procesa je osigurati da se podaci čuvaju u obliku koji omogućava identifikaciju ispitanika samo onoliko dugo koliko je to potrebno za svrhu za koju su ti osobni podaci prikupljeni, a nakon toga podaci se brišu ili anonimiziraju.

Pravni poslovi, uz podršku Službenika za zaštitu podataka, utvrđuju maksimalno razdoblje pohrane za svaku vrstu obrade u skladu s relevantnim zakonskim odredbama.

U slučaju nove obrade, ova se procjena provodi u procesu Privacy by Design, a razdoblje čuvanja podataka bilježi se u Evidenciji aktivnosti obrada.

Ako je brisanje/anonimizacija tehnički previše složena ili skupa, podaci se mogu pohraniti u aplikacijama s ograničenim pristupom.

Službenik za zaštitu podataka, putem informacija u Evidenciji aktivnosti obrade, nadzire zakonske rokove čuvanja podataka te provjerava provođenje potrebnih mjera za odvajanje.

Službenik za zaštitu podataka, putem naznaka u evidenciji o aktivnostima obrade, nadzire rokove za zakonske rokove pohrane, provjeravajući provedbu potrebnih mjera segregacije.

4.8 *Pravo pristupa podacima*

Uspostava svakog novog poslovnog procesa ili njegove izmjene, koja uključuje obradu osobnih podataka, zahtijeva procjenu funkcija odgovornih za obradu podataka i ovlasti pristupa u skladu s dodijeljenim zadatkom. Također je potrebno procijeniti inherentni rizik te odrediti mitigacijske mjere kroz ograničenja pristupa i sustav kontrola.

Ovom procjenom koordiniraju Ljudski resursi i Organizacija, a sudjeluju relevantne poslovne i pomoćne funkcije poput Službenika za zaštitu podataka i Korporativne sigurnosti u skladu s njihovim nadležnostima.

Mitigacijske mjere koje treba razmotriti prilikom procjene definirani su s obzirom na sljedeća opća načela:

- pristup podacima definira se prema logici minimizacije, odnosno ograničavanjem pristupa podacima samo osobama koje su ovlaštene sukladno definiranim pravilima i kojima su podaci potrebni za obavljanje konkretnih zadataka uz dodatnu kontrolu vidljivosti podataka ovisno o njihovoj ulozi;
- ovlaštenim osobama je pristup podacima dopušten isključivo u slučaju opravdane potrebe koja se može dokazati;
- pristup podacima ispitanika koji obavljaju ključne državne funkcije (npr. zakonodavne, pravosudne ili izvršne funkcije) i/ili funkcije važne za nacionalnu sigurnost (tzv. SEC klijenti) podliježe pojačanim sigurnosnim mjerama.

Opća načela moraju biti predmetom formaliziranih uputa i moraju se dostaviti trećim stranama (dobavljačima) koji su identificirani kao izvršitelji obrade osobnih podataka za Društvo, putem odgovarajućih ugovornih odredbi i kontrola propisanih člankom 28. GDPR-a.

4.9 Plan postupanja u slučaju neusklađenosti

Službenik za zaštitu podataka upravlja slučajevima neusklađenosti, pružajući pomoć i suradnju nadležnom organizacijskom dijelu, kako bi osigurao identifikaciju i provedbu radnji usmjerenih na otklanjanje ili ublažavanje posljedica slučaja, te identificirao sve organizacijske i/ili proceduralne nedostatke i s njima povezane mitigacijske mjere.

Poslovne funkcije i funkcije potpore pružaju podršku Službeniku za zaštitu podataka u upravljanju događajima neusklađenosti, osiguravajući identifikaciju i provedbu potrebnih mitigacijskih mjera.

Ako događaj neusklađenosti predstavlja povredu podataka (Data Breach), odnosno sigurnosni incident koji podrazumijeva povredu povjerljivosti, dostupnosti ili integriteta osobnih podataka, Službenik za zaštitu podataka procjenjuje koliki je njegov utjecaj na prava i slobode pojedinaca radi ispunjavanja obveza obavješćavanja nadzornog tijela i obavješćavanja ispitanika.

Upravljanje povredom podataka dio je šireg procesa upravljanja kritičnim događajima, kako to propisuju posebni interni akti. 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 obavijestiti uključene ispitanike kako bi im pružio informacije navedene u članku 34. GDPR-a, uključujući precizne informacije o mjerama koje preporučuje Društvo 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 država članica EU 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 povredu.

Ako povreda uključuje više voditelja obrade, svaki od njih obavještava svoje 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, mitigacijske postupke te ako je potrebno, razloge neuspjeha obavješćavanja. Registar je dostupan nadzornom tijelu u slučaju istrage.

4.10 Informiranje ispitanika te pribavljanje privola

Cilj procesa je prenijeti ispitanicima sve informacije potrebne za osiguranje točne i transparentne obrade putem informacija koje su sažete, transparentne, razumljive, lako dostupne, te napisane jednostavnim i jasnim jezikom.

Službenik za zaštitu podataka, uz podršku Pravnih poslova, priprema obavijest s općim informacijama i pripadajuće privole za svaku vrstu ispitanika čiji se podaci obrađuju (npr. klijenti, potencijalni klijenti, zaposlenici itd.), kao i obavijest s posebnim informacijama i pripadajuće privole, kad god je to potrebno za novu posebnu obradu koja je identificirana kroz proces identifikacije i metodologije obrade te sigurnosnim mjerama.

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 metodologije 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 Društvom)
- ako podaci nisu prikupljeni izravno od ispitanika:
 - informacije se dostavljaju u razumnom roku, no najkasnije unutar mjesec dana od prikupljanja osobnih podataka;
 - ako se osobni podaci koriste za komunikaciju s ispitanikom, informacija se dostavlja prilikom prve komunikacije s dotičnim ispitanikom;
 - ako se predviđa otkrivanje podataka drugim primateljima, informacija se dostavlja najkasnije do trenutka kad se osobni podaci prvi put otkriju.

Informacija se ispitaniku ne dostavlja ako i u onoj mjeri u kojoj:

- ispitanik već posjeduje tu informaciju;
- dostava takve informacije je nemoguća ili bi zahtijevala nerazmjeran napor;
- dobivanje ili otkrivanje tih informacija izričito je predviđeno zakonom EU ili pravom države članice kojemu podliježe voditelj obrade;
- osobni podaci moraju ostati povjerljivi radi obveze profesionalne tajne ili povjerljivosti regulirane pravom EU ili države članice.

Privole prikupljene prije stupanja na snagu Uredbe ostat će na snazi ako su dane na način koji je u skladu s uvjetima iz Uredbe.

4.11 Upravljanje pravima ispitanika

Cilj ovog procesa je osigurati učinkovito ostvarivanje prava koja Uredba pruža ispitanicima:

- a) pravo na pristup, tj. pravo dobivanja potvrde obrađuju li se osobni podaci ili ne, te ako se obrađuju, pravo na pristup tim podacima ili na dobivanje kopije podataka;
- b) pravo na ispravak/dopunu obrađenih podataka kako bi se osiguralo da su oni uvijek točni i ažurni;
- c) pravo na brisanje osobnih podataka koji su predmet obrade;

- d) pravo na ograničenje obrade tijekom određenog vremenskog razdoblja kako bi se zaštitila prava ispitanika;
- e) pravo na prijenos podataka, tj. pravo na:
 - 1. primanje osobnih podataka koje Društvo obrađuje i njihovo spremanje kako bi se mogli ponovno koristiti za osobne svrhe;
 - 2. prijenos osobnih podataka drugom voditelju obrade;
- f) pravo na prigovor na obradu koja se temelji na legitimnom interesu voditelja obrade;
- g) pravo na opoziv privole, koje mora biti moguće ostvariti jednako jednostavno kao i davanje privole;
- h) pravo na ljudsku intervenciju u slučajevima kada se donošenje odluka temelji isključivo na automatiziranoj obradi, izražavanje mišljenja, dobivanje objašnjenja o donesenoj odluci i osporavanje odluke;
- i) pravo na podnošenje pritužbe Nadzornom tijelu za zaštitu podataka, ne dovodeći u pitanje pravo ispitanika na žalbu bilo kojem drugom administrativnom ili sudskom tijelu, ako smatraju da obrada njihovih osobnih podataka od strane voditelja obrade krši Uredbu i/ili važeće zakonodavstvo.

Službenik za zaštitu podataka dužan je, u roku od mjesec dana od primitka zahtjeva, dati pisani odgovor ispitaniku ili ga, također u pisanom obliku, obavijestiti da će zbog složenosti zahtjeva odgovor biti dostavljen u roku od sljedeća dva mjeseca.

Ako nije moguće utvrditi identitet ispitanika na temelju zahtjeva, Službenik za zaštitu podataka može zatražiti dodatne dokaze (ovisno o korištenim kanalima, predočenje ili slanje kopije važećeg identifikacijskog dokumenta). U tom slučaju, vrijeme za odgovor počinje teći od trenutka primitka dodatne dokumentacije za potrebe utvrđivanja identiteta.

4.12 Aktivnosti nadzora i provjere usklađenosti (Assurance)

Praćenje rizika neusklađenosti sa zakonodavstvom koje se odnosi na zaštitu osobnih podataka uključuje definiranje odgovarajućih mjera za usklađenost sa zakonodavstvom i pravima ispitanika već od faze dizajna obrade, kao i naknadne provjere primjerenosti i stvarne primjene procesa, unutarnjih procedura i predloženih organizacijskih promjena te kontrolu stvarne usklađenosti s vanjskim i unutarnjim propisima od strane organizacijskih funkcija.

U tom kontekstu:

- Poslovne funkcije i funkcije podrške, uz pomoć relevantnih kontrolnih funkcija (u skladu s ciljevima kontrola koje postavlja Službenik za zaštitu podataka), definiraju kontrole prve razine i dostavljaju ih Službeniku za zaštitu podataka koji procjenjuje njihovu prikladnost za postizanje ciljeva kontrole te, gdje je to potrebno, zahtijeva njihovo usklađivanje;
- Službenik za zaštitu podataka definira kontrole druge razine koje se odnose na zaštitu podataka, određujući ciljeve, učestalost i metode provođenja;
- Unutarnja revizija definira kontrole treće razine koje se na to odnose.

Na temelju definiranih kontrola, poslovne funkcije i funkcije podrške te Službenik za zaštitu podataka provode kontrole prve i druge razine te ih dokumentiraju kroz izvješća pripremljena na temelju specifičnog obrasca koji sadrži sljedeće:

- karakteristike aktivnosti (svrha kontrole, primjenjivi unutarnji/vanjski regulatorni kontekst);
- detalje provedenih kontrola i pripadajuće rezultate;
- kratka razmatranja o preostalim rizicima i predložene mjere za njihovo ublažavanje.

Poslovne funkcije i funkcije podrške odgovorne su za planiranje i usvajanje mitigacijskih mjera.

Službenik za zaštitu podataka nadzire i prati napredak u provedbi identificiranih mjera.

4.12.1 Interakcije s ostalim kontrolnim funkcijama

U provedbi kontrola usklađenosti s propisima o zaštiti osobnih podataka, Službenik za zaštitu podataka koristi rezultate kontrola funkcija Društva zaduženih za nadzor kontrola druge i treće razine. Postupci suradnje između kontrolnih funkcija Društva i povezani informacijskih tokova opisani su u „Pravilniku o integriranom sustavu internih kontrola“

4.12.2 Proces praćenja

Službenik za zaštitu podataka, isključivo u regulatornim područjima koji pripadaju njegovom djelokrugu, redovito prati provođenje mjera za ublažavanje rizika koje su donesene kako bi se riješili ključni problemi utvrđeni kontrolama. U tu svrhu koriste se posebno definirani mehanizmi koji ovise o važnosti utvrđenih ključnih pitanja, kao i odgovarajući alati za praćenje napretka aktivnosti i promjena u identificiranim nedostacima. U slučaju značajnih kašnjenja, poduzimaju se potrebne eskalacijske mjere.

4.13 Širenje kulture privatnosti

Njegovanje kulture na svim razinama Društva, koja se temelji na poštivanju zakonitosti, pravičnosti, transparentnosti i pravilnog postupanja s podacima ispitanika, ključno je za učinkovito upravljanje rizicima povezanim sa zaštitom osobnih podataka.

Službenik za zaštitu podataka, uz podršku Ljudskih resursa i Organizacije te uz asistenciju odabranog vanjskog izvođača:

- godišnje definira i ažurira plan edukacije za zaposlenike vezano uz zaštitu osobnih podataka;
- priprema i odobrava materijale za edukaciju;
- prati sudjelovanje na edukacijama i rezultate prolaznosti.

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:

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

4.14 Odnosi s nadzornim tijelima

4.14.1 Odnosi s nadzornim tijelima

Službenik za zaštitu podataka surađuje s nadzornim tijelom, 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 prigovorima koje klijenti podnose AZOP-u te dostavlja odgovarajuće odgovore AZOP-u i ispitaniku;
- dostavlja kontakt podatke Službenika za zaštitu podataka nadzornim tijelima.

4.14.2 Zahtjevi nadzornih tijela iz treće zemlje

Zahtjevi koji se odnose na osobne podatke, a koje upućuju regulatorna tijela treće zemlje ili zemlje izvan Europske unije, prosljeđuju se 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);
- javni interes priznat zakonom države u kojoj voditelj obrade ima poslovni nastan koji zakonom dopušta takav prijenos osobnih podataka.

Samo ako je ispunjen barem jedan od gore navedenih uvjeta, Službenik za zaštitu podataka, uz asistenciju Pravnih poslova, može odobriti prijenos te o tome obavještava nadležno regulatorno tijelo treće zemlje.

4.15 Informacijski tokovi prema korporativnim tijelima

Korporativna tijela na razini PBZC primaju periodična izvješća o učinkovitosti i primjerenosti nadzora usklađenosti s propisima o zaštiti osobnih podatak.

Izvješća priprema Službenik za zaštitu podataka i uključuju:

- godišnje izvješće koje sažima provedene aktivnosti i planiranje postupaka u skladu s GDPR-om te obavijest o osobito važnim pitanjima zaštite podataka;
- informacije o svakom problemu u poslovanju Društva koja proizlaze iz povreda osobnih podataka, dostupnosti ili integriteta.

5 SMJERNICE I KOORDINACIJA PBZ GRUPE

Kao društvo unutar PBZ Grupe, koje posluje u skladu sa Smjernicama Grupe o zaštiti osobnih podataka fizičkih osoba donesenima na razini Intesa Sanpaolo Grupe, PBZ Card primjenjuje upute i metodologije definirane od strane matičnog društva (PBZ d.d.).

Službenik za zaštitu podataka u PBZ Card d.o.o. dužan je:

- osiguravati i poticati primjenu Grupnih smjernica o zaštiti osobnih podataka fizičkih osoba te Politike PBZ-a o zaštiti osobnih podataka, uz njihovu prilagodbu, prema potrebi i u koordinaciji sa Službenikom za zaštitu podataka matičnog društva, specifičnostima lokalnog regulatornog okvira te poslovnim, geografskim i organizacijskim obilježjima Društva;
- provoditi operativne procese definirane od strane matičnog društva te surađivati s istim u vezi svih potrebnih usklađivanja s konkretnim poslovnim kontekstom Društva;
- pravodobno dostavljati matičnom društvu sve tražene informacije u području zaštite osobnih podataka te bez odgode izvještavati o svim značajnim događajima koji mogu imati utjecaj na usklađenost;
- na zahtjev nadležnog za usklađenost matičnog društva dostavljati tromjesečna izvješća te, prema potrebi, sudjelovati u mjesečnim koordinacijskim aktivnostima.

Službenik za zaštitu podataka Matičnog društva (PBZ d.d.):

- nadzire ispravnu primjenu smjernica i propisa Grupe o zaštiti osobnih podataka unutar PBZ Grupe;
- pruža stručnu podršku u zaštiti osobnih podataka;
- na zahtjev, pruža podršku članicama PBZ Grupe u odnosima s nadležnim tijelima.

6 DEFINICIJE

“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).

“Nadležno 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

“Ovlašteni subjekt”: fizička osoba koju su voditelj obrade ili izvršitelj obrade ovlastili za izvršavanje obrade. Na primjer, zaposlenici Društva prilikom obavljanja svojih radnih aktivnosti moraju konzultirati osobne podatke klijenata ili dobavljača.

“Privola ispitanika”: svaka slobodno dana, posebna, informirana i nedvosmislena izjava volje ispitanika kojom on ili ona daje suglasnost za obradu svojih osobnih podataka izjavom ili jasnim potvrdnim radnjama.

“Zajednički voditelji obrade”: dva ili više voditelja obrade koji zajednički određuju svrhe i sredstva obrade.

“Službenik za zaštitu podataka (DPO)”: osoba odgovorna za zaštitu osobnih podataka utvrđena prema GDPR-u.

“Osobni podaci”: svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, uključujući obrtnike 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 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 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.

“Privatnost u dizajnu” (Privacy by Design): načelo zaštite podataka od samog početka, odnosno načelo prema kojemu voditelj obrade usvaja odgovarajuće tehničke i organizacijske mjere, poput pseudonimizacije, s ciljem učinkovite primjene načela zaštite podataka, kao što su načela minimizacije, uključujući potrebne sigurnosne mjere u obradi kako bi se ispunili zahtjevi GDPR-a i

zaštitila prava ispitanika. Prilikom provođenja ovih aktivnosti, voditelj obrade uzima u obzir tehnološka dostignuća i troškove provedbe, kao i prirodu, primjenu, kontekst i svrhe obrade, kao i rizike s različitim vjerojatnostima i ozbiljnošću obrade za prava i slobode fizičkih osoba, prilikom određivanja načina obrade i tijekom same obrade.

“Privatnost prema zadanim postavkama” (Privacy by Default): načelo zaštite podataka prema zadanim postavkama, tj. načelo prema kojem voditelj obrade usvaja tehničke i organizacijske mjere koje su primjerene kako bi se osiguralo da se obrađuju samo osobni podaci potrebni za svaku specifičnu svrhu obrade. Ova obveza odnosi se na količinu prikupljenih osobnih podataka, opseg obrade, razdoblje čuvanja i dostupnost. Mjere jamče da osobni podaci nisu dostupni neograničenom broju fizičkih osoba. Jedna procjena može se odnositi na skup sličnih aktivnosti obrade s ekvivalentno visokim rizicima.

“Procjena učinka na zaštitu podataka (Data Protection Impact Assessment-DPIA): procjena učinka na zaštitu podataka, koja se unaprijed provodi kada neka vrsta obrade može predstavljati visoki rizik za prava i slobode fizičkih osoba, temeljem primjene novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade.

“Automatizirani proces odlučivanja”: 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 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.

“Evidencija aktivnosti obrade”: pisana ili elektronička evidencija koju vodi voditelj obrade, a koja sadrži informacije o obradi koja se provodi pod njegovom odgovornošću. Izvršitelj obrade također vodi evidenciju koja sadrži informacije o svim kategorijama aktivnosti povezanim s obradom provedenom u ime voditelja obrade.

“Izvršitelj obrade”: fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade. Izvršitelj obrade obično je treća strana izvan Društva. U slučaju grupe društava, jedno društvo može djelovati kao izvršitelj obrade i za druga društva grupe: na primjer, u kontekstu Intesa Sanpaolo Grupe ili PBZ Grupe, podružnica može, na temelju ugovora o pružanju usluga, imenovati druga društva unutar Grupe kao izvršitelje obrade. Obveze izvršitelja obrade s voditeljem obrade moraju biti specificirane u ugovoru ili drugom pravnom dokumentu.

"Glavni poslovni nastan": a) što se tiče voditelja obrade s poslovnim nastanima u više od jedne države članice, mjesto njegove središnje uprave u EU, osim ako se odluke o svrhama i sredstvima obrade osobnih podataka donose u drugom poslovnom nastanu voditelja obrade u EU 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 ili ako izvršitelj obrade nema središnju upravu u EU, 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 ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom EU ili pravom države članice. Voditelj obrade odlučuje "zašto" i "kako" se osobni podaci moraju obrađivati, dok zaposlenici koji obrađuju osobne podatke unutar Društva djeluju kako bi obavili dužnosti voditelja obrade Društva. U kontekstu Intesa Sanpaolo Grupe ili PBZ Grupe, svako društvo je voditelj obrade osobnih podataka koje prikuplja izravno za vlastite svrhe.

"Obrada podataka": 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 podataka": znači ili: a) obrada osobnih podataka koja se odvija u EU 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 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": znači sigurnosni incident koji dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili obrađeni na neki drugi način.