Cilj ove politike je da definiše namenu, smernice, uspostavi principe i osnovna pravila za menadžment informacione bezbednosti kada je u pitanju upravljanje podacima o ličnosti. Ovom politikom rukovodstvo kompanije Saga d.o.o. Beograd (daje u tekst Saga) određuje stav organizacije prema podacima o ličnosti, definiše pravila, dodeljuje odgovornosti i daje punu podršku sistemu upravljanja podacima o ličnosti. Podaci o ličnosti koje Saga prikuplja i obrađuje u svom radu smatraju se poverljivom informacionom imovinom koja je kompaniji ustupljena od strane njihovih vlasnika. Ovim se podacima mora postupati sa posebnom pažnjom, a dozvoljeno je da se koriste isključivu u skladu s razlogom iz kojeg su prikupljeni.
Kompanija Saga primenjuje **osnovne principe** za menadžment obrade, korišćenja, skupljanja i prenosa ličnih (personalnih podataka), koji se zahtevaju primenljivim zakonima:

1. Lični podaci će se procesirati samo u skladu sa zakonom i standardima najbolje prakse.
2. Lični podaci će se prikupljati samo za specifične, eksplicitne, zakonske i legitimne namene i neće biti dalje procesirani ni na jedan način koji nije u skladu sa ovim namenama.
3. Lični podaci će biti adekvatni, relevantni i minimalni u odnosu na namenu za koju su skupljani i/ili procesirani.
4. Lični podaci će biti tačni, kompletni i aktuelni za namenu za koju su skupljani i/ili procesirani.
5. Lični podaci ne smeju se čuvati u formi koja dopušta identifikaciju vlasnika podataka (subjekta), ne dalje nego što je potrebno za izvršavanje namenjene funkcije.
6. Lični podaci se neće obradjivati, skupljati ili procesirati, osima ako:
   - vlasnik podataka nije obezbedio (dostavio rukovaocu) validnu informaciju o pristanku;
   - procesiranje nije neophodno za izvršavanje ugovora čiji je vlasnik podataka sastavni deo, ili da bi se preduzeli koraci po zahtevu vlasnika pre ulaska u ugovorne obaveze;
   - procesiranje nije neophodno za usaglašavanje sa legalnim obavezama poslovnog sistema;
   - procesiranje nije neophodno da bi se zaštitili vitalni interesi vlasnika podataka;
   - procesiranje nije neophodno za izvršavanje zadataka od javnog interesa, ili za rad revizora zaštite podataka (kontrolora), ili poverljive treće strane kojoj su podaci otkriveni,
   - procesiranje nije neophodno za legitimne interese poslovnog sistema, partnera ili treće strane kojoj su podaci otkriveni, osim ako takvi interesi nisu u sukobu sa fundamentalnim pravima i slobodama vlasnika podataka.
7. Lični podaci će se skupljati i pocesirati u skladu sa pravima vlasnika podataka.
8. Odgovarajuće fizičke, tehničke i proceduralne kontrole (mere) zaštite će biti preduzete da:
   spreče i/ili identifikuje neovlašćeno ili nezakonito skupljanje, procesiranje i prenos personalnih podataka, i spreče slučajni gibitak, objavljivanje ili destrukciju, ili oštećenje personalnih podataka.

Prikupljanje podataka o ličnosti se sme sprovoditi isključivo u skladu sa zakonskim propisima i etičkim načelima. Podatke o ličnosti je dozvoljeno obrađivati samo kada za to postoji jasno određena i dokumentovana zakonska osnova ili osnova ugovornog odnosa, dok su sve ostale obrade podataka o ličnosti dozvoljene jedino uz jasno dokumentovan pristanak njihovog vlasnika ili njegovog opunomoćenika.
Prilikom prikupljanja i obrade podataka o ličnosti, obavezna je primena načela prema kojem je dozvoljeno da se prikupljaju samo oni podaci koji su za predmetnu obradu stvarno i potrebni.
Svako prikupljanje suvišnih podataka je zabranjeno.
Pre prikupljanja podataka o ličnosti, vlasnicima se mora pružiti jasna informacija o razlogu prikupljanja, vrsti obrade u kojoj će se informacije koristiti, te eventualnim trećim osobama koje će informacijama pristupati.
Ako se podaci prikupljaju od dece, neophodno je uspostaviti posebne mehanizme koji će osigurati da su deca dovoljno stara kako bi razumela posledice davanja informacija. Svakom prikupljanju i obradi informacija maloletnika mora se pristupati sa posebnom pažnjom, te se pri tome mora voditi najvišim etičkim načelima.
Svi zaposleni ili eksterno angažovana lica koja imaju poslovnu potrebu ili mogućnost pristupa podacima o ličnosti u Sagi ili kod korisnika, moraju da imaju definisane Ugovore, klauzule ili personalne Izjave o poverljivosti, koje definišu personalne odgovornosti u cilju zaštite podataka o ličnosti.
Sve eksterno angažovane kompanije moraju da imaju potpisane NDA ugovore o saradnji kao i odgovarajuće personalne Izjave o poverljivosti u slučaju da se radi i pristupa podacima o ličnosti.

PRAVA VLASNIKA PODATAKA O LIČNOSTI

Vlasnicima podataka o ličnosti mora se omogućiti pravo na pristup informacijama o tome koje podatke o ličnosti Saga o njima poseduje i zašto se koriste. Saga vlasniku podataka o ličnosti mora omogućiti ispravku netačnih i nadopunu nedostajućih podataka o ličnosti, te mogućnost uskraćivanja prava na obradu njegovih podataka kada se obrada zasniva na pristanku vlasnika (pravo na ispravku, transfer ili zaborav).
Na zahtev vlasnika, podatke o ličnosti koje su date na osnovu pristanka moraju se obrisati iz svih informacionih sistema Organizacije i informacionih sistema trećih strana kojima je Saga omogućila pristup ovim podacima.
Vlasnik ima pravo na prenosivost svojih podataka o ličnosti. Na zahtev vlasnika, njegovi se podaci o ličnosti moraju isporučiti u elektronskom obliku.

EVIDENCIJA, ČUVANJE I POSTUPANJE

Saga je uspostavila i dužna je da održava registar vrsta podataka o ličnosti i obrada koje se nad njima sprovode (Data Protection Impact Assessment - DPIA), a za svaku obradu i vrstu podataka o ličnosti imenuje odgovornu

organizacionu jedinicu ili osobu. Odgovorna osoba je dužna da osigura da se u obradu uključuju isključivo podaci o ličnosti za čiju obradu postoji odgovarajući pristanak, zakonska osnova ili poslovna potreba. Svi podaci o ličnosti za koje ne postoji osnova čuvanja, moraju se bez odlaganja uništiti.

Kompanija Saga je dužna da podatke o ličnosti adekvatno osigura tehničkim i organizacionim merama. Podaci o ličnosti se u treće zemlje smeju slati isključivo u skladu sa dozvolom regulatora ili Rukovaoca u skladu sa regulativom koja je uspostavljena na nivou EU, te ukoliko je moguće osigurati regulativom određeni nivo sigurnosti.

Kod izgradnje informacionih sistema i dizajna poslovnih procesa koji na bilo koji način mogu uticati na sigurnost podataka o ličnosti ili ostvarivanje prava na privatnost njihovih vlasnika, Saga će sprovoditi procenu uticaja na sigurnost te osigurati primerene zaštitne mere. Ukoliko ustanovi da zaštitne mere koje može implementirati nisu dovoljne, pre obrade će se savetovati s nadležnim telom. Svi novi procesi i informacioni sistemi u kompaniji moraju se dizajnirati tako da ispunjavaju sve zahteve ove Politike.

MINIMIZACIJA I ZAŠTITA PODATAKA O LIČNOSTI

Saga podatke o ličnosti prikuplja i skladišti isključivo u meri u kojoj je to potrebno za pružanje usluge. Prilikom skladištenja podataka, podaci o ličnosti će se arhivirati na najmanjem mogućem broju mesta na kojima moraju biti adekvatno zaštićeni. Pristup podacima o ličnosti je omogućaen isključivo na osnovu poslovne potrebe i definisanih prava pristupa.
Zabranjeno je koristiti podatke o ličnosti u svrhe razvoja ili testiranja IT sistema.
Gde god je to moguće, podaci o ličnosti moraju biti zaštićeni:

- enkripcijom,
- pseudonimizacijom ili
- anonimizacijom.

Kompanija Saga je uspostavila tehničko aplikativne sisteme zaštite lokalne ICT infrastrukure sa ciljem očuvanja Poverljivosti, Integriteta i Raspoloživosti informacija a posebna pažnja će se voditi o podacima o ličnosti koji se nalaze na lokalnoj ICT infrastrukturi. Takodje, neophodno je kontinuirano razmatrati bezbednosna unapredjenja u cilju minimalizovanja rizika od odliva ili kompromitacije podataka o ličnosti na ICT infrastrukturi i blagovremeno ukazivati na moguće rizike i poboljšanja. Neizostavno je obezbeđivanje trajne poverljivosti, integriteta, raspoloživosti i otpornosti sistema i usluga obrade u skladu sa zahtevima Rukovaoca. Kao i obezbeđivanje uspostavljanja ponovne raspoloživosti i pristupa podacima o ličnosti u slučaju fizičkih ili tehničkih incidenata u najkraćem roku u skladu sa zahtevima Rukovaoca i definisanim SLA parametrima iz Ugovora u saradnji sa Tehničkom podrškom.

UPRAVLJANJE INCIDENTIMA

Saga ima implemnetirane procedure odgovora na incidente vezane uz narušavanje sigurnosti podataka o ličnosti, kako unutar kompanije, tako i kod trećih strana kojima je Saga ustupila ili koje su organizaciji ustupile podatke o ličnosti. Saga ima uspostavljenu strukturu odgovornosti za izveštavanje o incidentima vezanim uz sigurnost podataka o ličnosti koja se redovna prati i održava.
Svaki zaposleni je u obavezi da poštuje osnovne principe zaštite podataka o ličnosti definisane aktulenom verzijom Zakona o zaštiti podataka o ličnosti u slučaju identifikovanja slabosti ili incidenta po pitanju ugrožavanja bezbednosti podataka o ličnosti i obaveznu prijavi na email adresu dpo@saga.rs.

Saga je uspostavila i održava mere za detekciju neovlašćenog pristupa podacima o ličnosti i curenja podataka o ličnosti iz informacionog sistema.
U slučaju narušavanja sigurnosti podataka o ličnosti, Saga će bez odlaganja, a najkasnije u roku od 72 sata po otkrivanju incidenta, o tome izvestiti nadležno telo. U slučaju curenja podataka o ličnosti, Saga će o tome obavestiti i vlasnike čiji su podaci kompromitovani ukoliko se to može sprovesti na razuman način, ukoliko su ti podaci čitljivi trećoj neautorizovanoj strani.
Uspostavljen je proces obavezujućeg potpisivanja Izjave o poverljivosti sa definisanim obavezema i odgovornostima.

Kada su podaci Saginih zaposlenih u pitanju ukoliko se desi Incident koji uključuje podatke o ličnosti pokreće se preispitivanje od strane kompanije kao sastavni deo procesa menadžmenta incidentima narušavanja bezbednosti informacija, kako bi se utvrdilo da li je došlo do narušavanja podatke o ličnosti koje zahteva odgovor. Događaj ne mora nužno da pokrene takvo preispitivanje.

Kada se putem postupak preispitivanja incidenta utvrdi da je došlo do narušavanja podataka o ličnosti, procedurom odgovora na incident bezbednosti informacije pristupa se evidentiranju događaja i izradi odgovarajućih obaveštenja. kao što su:

– tačka kontakta gde se može dobiti više informacija
– opis i moguće posledice narušavanja;
– opis narušavanja, uključujući broj zainteresovanih lica, kao i broj zapisa;
– preduzete ili planirane mere u cilju minimalizovanja rizika

Izuzetno, uz postojanje opravdanog razloga, a na zahtev zainteresovanih strana, Službenik za zaštitu podataka o ličnosti može odobriti privremeno postupanje sa podacima o ličnosti koje nije u skladu s ovom Politikom uz informisanje najvišeg rukovodstva. Službenik za sigurnost podataka o ličnosti dužan je da vodi evidenciju ovakvih odobrenja, odgovornosti i rokova za usklađivanje, te o tome izveštava delegirano rukovodstvo.

Svaki zaposleni Sage koji u poslovnim aktinostima pristupa ili održava infrastrukturu korisnika – Rukovaoca, u obavezi je da se pridržava navedenih smernica koje su definisane osnovnim odredbama Zakona kao i potpisanih Ugovora o obradi podataka sa korisnicima (Data Processing Agreement - DPA).

Privatnost sa dizajnom je eksplicitan legalni zahtev, pa je važno razmatrati kako ugraditi privatnost u poslovne procese i aktivnosti koje su neophodne za razvoj softvera. Neophodno je vršiti analizu zahteva korisnika i moguću procenu uticaja privatnosti na nivou zahteva korisnika i neophodnih elemenata za zaštitu podataka o ličnosti u aplikaciji ili softveru.

Za uspostavljanje i održavanje sistema upravljanja podacima o ličnosti, te koordinaciju tima i delegiranih organizacionih jedinica i aktivnosti vezanih za upravljanje podacima o ličnosti odgovoran je Službenik za zaštitu podataka o ličnosti (Data Protection Officer - DPO) , Menadžer bezbednosti inforamacija, Sektor za pravne poslove i Odeljenje Integrisanih sistema menadžmenta. Ova se politika revidira najmanje jednom godišnje ili nakon svake izmene u pravnom okruženju ili okruženju rizika koja bi mogla imati uticaj na njenu efektivnost.

Ova Politika je prihvaćena od strane najvišeg rukovodstva i obavezujuća je za sve zaposlene u organizaciji kao i sve angažovane podizvođače i konsultante na projektima koji su odgovorni za njenu primenu. Politika se primenjuje integrisano sa Politikom sistema menadžmenta bezbednosti inforamacija, kao i ostalim politikama u organizaciji.

Direktor