OPŠTI USLOVI ZA OSIGURANJE USKLAĐENOSTI U VEZI SA INFORMACIONIM REŠENJIMA I INFORMACIONIM USLUGAMA

1 UVODNE ODREDBE

Član 1

(1) Opšti uslovi Halcom a.d. za osiguranje usklađenosti sa informacijskim rešenjima i informacijskim uslugama (u daljem tekstu: opšti uslovi), definišu uslove partnerstva, kao i prava i obaveze pružaoca ili dobavljača Halcom a.d. (u daljem tekstu: Halcom ili pružalac) i kupca ili klijenta (u daljem tekstu: klijent), u pogledu zaštite podataka (podaci o ličnosti, poslovne tajne), usklađenosti procesa i rešenja i drugih ovlašćenja u skladu sa važećim srpskim propisima i međunarodnim i evropskim tehničkim standardima i preporukama.

(2) Opšti uslovi imaju karakter ugovora i čine njegov sastavni deo, dopunjuju ga i obavezuju ugovorne strane na isti način kao i ugovor. Sklapanjem ugovora sa Halcom a.d. klijent izjavljuje da je upoznat sa sadržajem opštih uslova i prihvata sadržaj u celosti. Ako su uslovi ugovora različiti od ovih opštih uslova, važe uslovi ugovora sa klijentom.

(3) Halcom će prilikom potpisivanja ugovora dostaviti elektronsku kopiju opštih uslova. Opšti uslovi su, takođe, dostupni u sedištu Halcoma i na web-stranici Halcoma.

Član 2

(1) Strane su saglasne da obezbede, u skladu sa pravilima o zaštiti podataka o ličnosti, uslove i mere za obezbeđivanje zaštite podataka o ličnosti i da spreče moguće zloupotrebe, u skladu sa odredbama važećih propisa.

(2) Halcom izjavljuje da ima registrovanu aktivnost obrade podataka u skladu sa opštom klasifikacijom aktivnosti ili drugim odgovarajućim aktivnostima, koje zahtevaju važeća pravila o zaštiti podataka kao uslov za obavljanje ugovorne obrade podataka o ličnosti.

(3) Halcom će obraditi lične podatke u ime klijenta u skladu sa propisima Republike Srbije, međunarodnim i evropskim standardima i drugim pravilima struke, ovim ugovorom i uputstvima klijenta.

Član 3

(1) Za potrebe ovih opštih uslova, strana u otkrivanju određenih informacija naziva se "posrednik", a strana koja prima takve informacije je "strana koja prima informacije".

(2) "Poverljive informacije" u okviru ovih opštih uslova će označavati svaku poslovnu tajnu ili informacije komercijalne, finansijske i tehničke prirode i sve druge informacije koje stranka posrednica smatra poverljivim i one mogu da budu pripremljene u bilo kojoj formi, uključujući softver, analize, proračunske tablice, podatke, studije ili druga dokumenta koje priprema strana koja prima informacije na osnovu ili u vezi sa poverljivim informacijama. Poverljive informacije, takođe, podležu svim dokumentima koje strana primalac priprema na osnovu takvih informacija ili koje sadrže ili su u potpunosti ili delimično pripremljene na osnovu takvih informacija.

2 OVLAŠĆENJA ZA OBRADU PODATAKA O LIČNOSTI

Član 4

Klijent ovlašćuje Halcom da obrađuje lične podatke u skladu sa uslovima ugovora ili ovim opštim uslovima, koji su sastavni deo ugovornog odnosa.

Skup podataka:

a. detalje o bankovnom računu, uključujući (lično ime, adresu prebivališta, JMBG broj, imejl adresu, broj telefona, serijski broj autentifikacionog agenta i druge detalje zastupnika, autentikaciju i ovlašćenja);
b. aktivnosti, poruke i dokumenta zastupnika u elektronskoj banci (vreme povezivanja, IP adresa, sredstva za identifikaciju, izvršene radnje i poslate poruke ili dokument u elektronskoj banci);
c. aktivnosti, poruke i bankovna dokumenta (vreme povezivanja, IP adresa, sredstva za identifikaciju, primljene poruke ili dokumenta u elektronskoj banci);
d. revizioni tragovi (vreme aktivnosti, lično ili korisničko ime, podaci o aktivnosti ili unos, promena ili pristup podacima).

Svrha obrade: izvršenje platnih usluga i drugih usluga između klijenta i jedne ili više komercijalnih banaka, garantovanjem efikasnosti rada usluga i pružanjem informacione bezbednosti, kao i drugi poslovi u skladu sa ugovorom.

Vreme obrade: u skladu sa važećim propisima – 10 godina od transakcije po propisima o sprečavanju pranja novca i finansiranja terorizma; 3 ili 5 godina u skladu sa obaveznim rokom zastarevanja nakon prestanka ugovornog odnosa između klijenta i banke, ograničeno trajanjem ugovornog odnosa prema ovom ugovoru i aneksom. U skladu sa pravilima o zaštiti podataka, zakonom propisanim rokom zastarelosti, trag revizije čuva se 6 godina od datuma pojedinačnog informativnog događaja, mere ili transakcije.

Član 5

(1) Halcom može da obrađuje lične podatke isključivo u meri i samo u svrhe i u periodu određenom u ovlašćenju iz prethodnog člana.

(2) Nakon raskida ugovora ili u bilo koje vreme na zahtev klijenta, Halcom je dužan da osigura brisanje ili blokiranje podataka o ličnosti koje je primio ili obradio na osnovu ovlašćenja iz prethodnog člana u skladu s uslovima ugovora.

(3) Nakon raskida ovog ugovora ili u bilo koje vreme na zahtev klijenta, Halcom je dužan da klijentu dostavi sve ili deo podataka o ličnosti koje je primio ili obradio na osnovu ovlašćenja iz prethodnog člana u skladu sa uslovima ugovora.

(4) Obaveze iz ovog člana Halcom ne sme nikako uslovljavati, i Halcom je dužan da ih sprovodi bez obzira na status ugovornog odnosa, mogućeg spora

- sa klijentom ili bilo koje neizvršene obaveze klijenta. Halcom može odbiti da ispuni svoje obaveze samo ako je to predviđeno zakonom.

3 POSLOVNA TAJNA

Član 6

Sve poverljive informacije dobijene od stranke posrednika su vlasništvo te stranke ili nosioca prava intelektualne svojine, koje ta stranka priznaje.

. Prenos ovih informacija ne daje primaocu nikakva prava u odnosu na prenesene informacije.

Član 7

(1) Obaveze propisane ovim opštim uslovima ne odnose se na poverljive informacije koje:

- strana koja ih prima već poseduje pre nego što je primljena od strane posrednika;
- su ili postaju javne, ne iz nekog drugog razloga, osim zbog kršenja ovog ugovornog odnosa;
- strana koja ih je primila samostalno ih je razvila;
- strana primalac može, na osnovu pismenog odobrenja posrednika, proslediti trećoj strani;
- su primljene od trećeg lica bez sličnih ograničenja i bez kršenja ovog ugovornog odnosa;
- strana primalac dostavlja na zahtev nadležnog suda ili drugog državnog organa.

(2) U slučajevima posredovanja državnim vlastima, strana koja prima informacije će obavestiti drugu ugovornu stranu pre slanja tih informacija, tako da strana koja posreduje može preduzeti sve potrebne mere kako bi na odgovarajući način zaštitila svoja prava u pogledu traženih poverljivih informacija. U svakom slučaju, strana koja prima informacije mora dostaviti državnim organima samo onaj deo poverljivih informacija koji se zahteva po zakonu i koji se mora dostaviti i mora se uložiti svaki napor da od se od primaoca informacije dobije izjava o službenoj tajnosti ili drugom odgovarajućem jemstvu, da će dostavljene informacije biti tretirane kao poverljive;

(3) Izuzev gore navedenih tačaka, obaveze koje proističu iz ovih opštih uslova ostaju na snazi i nakon ostvarivanja poslovne svrhe ili prestanka ugovornog odnosa iz bilo kog razloga.

Član 8

(1) Ugovorne strane su saglasne da objave poverljive informacije i dostave ih jedna drugoj, u meri potrebnoj za ostvarivanje poslovne svrhe. Strane su saglasne da neće pružati poverljive informacije trećoj strani, bilo fizičkom licu, preduzeću, kompaniji, udruženju ili bilo kom drugom entitetu iz bilo kog razloga ili svrhe.

(2) Strankama je dozvoljeno da daju poverljive informacije svojim zaposlenima. Zaposleni mogu dobiti samo informacije koje su im potrebne u radu.

Član 9

(1) Strane su saglasne da neće bez izričitog pismenog, prethodno pisanog pristanka posrednika, koristiti, iskoristiti ili na bilo koji drugi način upotrebiti dostavljene poverljive informacije, osim za ostvarivanje poslovne svrhe.

(2) Strana koja prima informacije će ograničiti pristup poverljivim informacijama svojim zaposlenima, pružajući samo informacije potrebne za njihov rad. Neće pružati poverljive informacije drugim osobama, osim ako je izričito navedeno u ovim opštim uslovima ili ugovorom.

Član 10

(1) Strana posrednik može, u bilo kom trenutku da pismeno zatraži vraćanje bilo koje pismene poverljive informacije, dostavljene u skladu sa uslovima ovog ugovora, kao i bilo koje njihove kopije, zajedno sa pisanom izjavom od strane primaoca da nije svesno zadržao u svom vlasništvu ili pod njegovom kontrolom bilo koju poverljivu informaciju ili njenu kopiju. Primalac će ispuniti svoju obavezu da vrati poverljive informacije u roku od 8 (osam) dana od prijema takvog zahteva.

(2) Deo poverljivih infohrmacija koji se sastoji samo od analiza, proračunskih tablica, studija ili drugih dokumenata pripremljenih za stranku primaoca i koja se ne vraća posredniku u skladu s ovim sporazumom, uništiće se na njegov zahtev, što će stranka koja je primila pismeno i potvrditi.

Član 11

Svaka strana potvrđuje i garantuje drugoj strani da je osnovana i radi u skladu sa važećim propisima u zemlji u kojoj je osnovana. Svaka strana potvrđuje da je pravno valjano zaključila međusobni ugovor i pristala na ove opšte uslove da će izvršiti sve neophodne aktivnosti u vezi sa implementacijom ovog ugovornog odnosa. Posrednik garantuje da ne krši bilo koji drugi ugovor sa trećim stranama, pružajući poverljive informacije.

4 POUZDANOST OSOBLJA

Član 12

(1) Halcom garantuje da su samo pouzdani zaposleni uključeni u obradu podataka o ličnosti i moraju da ispunjavaju uslove:

- da su adekvatno verifikovani u procedurama **zapošljavanja**, a usklađenost sa propisanim uslovima se konstantno proverava;
- ugovorno ili posebnom izjavom u obavezi su da štite osetljive informacije;
- profesionalno su obučeni za svoj rad i stalno održavaju potrebni nivo znanja i veština.

(2) Halcom će zaposlenima omogućiti pristup podacima o ličnosti ili poverljivim informacijama, što je neophodno za njihov rad u vezi sa ugovornim zadacima. Takođe će osigurati da se osetljivi zadaci pravilno organizuju i sprovode odvojeno (podela i segregacija dužnosti), a kritični zadaci zahtevaju učešće najmanje dva ovlašćena i obučena radnika (princip četiri oka), i u najvećoj meri sprečava pojedinačne zaposlene da samostalno ugrožavaju bezbednost i integritet podataka o ličnosti ili poverljivih informacija.

(3) Strane se, takođe, slažu da se poverljive informacije, a ne nužno i podaci o ličnosti, mogu preneti i njihovim profesionalnim savetnicima i agentima, pod uslovom da potpišu izjavu o poverljivosti pod istim uslovima koji su sadržani u ovim opštim uslovima.

(4) Odredbe prethodnih stavova primenjuju se *mutatis mutandis* na spoljne saradnike ili zaposlene podugovarače, ako je saradnja sa njima odobrena od strane klijenta.

5 TEHNOLOŠKA SIGURNOST

Član 13

(1) Strane su saglasne da čuvaju poverljive informacije druge strane u skladu sa istim standardima zaštite informacija koje koriste, da bi zaštitile svoje poverljive informacije i da će delovati i postupati na takav način da spreče neovlašćeno otkrivanje takvih informacija.

(2) Halcom će koristiti međunarodno priznatu opremu priznatih proizvođača ili afirmisano otvoreno kodno rešenje i usluge utvrđenih i proverenih dobavljača (uzimajući u obzir kvalitet usluge, tehnološke kompetencije, finansijske bonitete i sl.) za obavljanje poslova iz ugovora i ovih opštih uslova.

(3) Halcom je obavezan da uspostavi efikasan sistem informacione bezbednosti u skladu sa međunarodnim standardima (ISO 27001), što je dokazano redovnim nezavisnim spoljnim proverama i validnim sertifikatom.

(4) Halcom može koristiti podugovarače u skladu sa odredbama člana 15 ovih opštih uslova, radi obavljanja ključnih zadataka po ugovoru ili zadataka koji mogu imati značajan uticaj na izvršavanje poslova iz ugovora ili zaštite podataka o ličnosti.

(5) Halcom je dužan da vodi spisak informacionih resursa (informacioni resursi, procena rizika, mere bezbednosti, odgovorno lice, itd.) i ažuriranu dokumentaciju o obavljenim radovima, instalacijama opreme, korisničkim imenima i lozinkama, inventaru opreme, kontakt osobu za svaku lokaciju.

(6) Svi radovi održavanja bilo kojeg hardvera moraju se obavljati na mestu gde se oprema nalazi. Ako to nije moguće, nosioci podataka sa opreme moraju biti uklonjeni i sigurno sačuvani. Ako se podaci ne mogu ukloniti ili na drugi način zaštititi, postupak održavanja mora biti nadziran. Nakon radova na održavanju, oprema mora biti pregledana pre puštanja u rad.

Član 14

Halcom garantuje sigurnost i čuvanje podataka u skladu sa svojim internim aktima i sigurnosnim politikama, u kojima pruža sve potrebne tehničke, organizacione i kadrovske procedure i mere za osiguranje informacione bezbednosti i zaštite podataka o ličnosti.

Interni akti ili bezbednosne politike pokrivaju najmanje sledeće obaveze:

- Halcom garantuje da su svi prostori u kojima se nalazi informacioni sistem ili njegovi delovi ili rezervne kopije podataka, kao i lični podaci na fizičkim ili elektronskim medijima, fizički ili elektronski zaštićeni;
- Halcom obezbeđuje fizičku i elektronsku bezbednost hardvera, sistema i aplikativnog softvera, uključujući ulazne i izlazne jedinice i bezbednost podataka o ličnosti na fizičkim ili elektronskim medijima u skladu sa principima bezbednosti informacija;
- Halcom obezbeđuje operativnu bezbednost (elektronska bezbednost i bezbednost mreže, bezbednost aplikacija, revizijski tragovi i sl.);
- Halcom obezbeđuje upravljanje identitetom i pristup (autoritet, identitet, upravljanje ključevima, enkripcija, autentifikacija, revizijski trag);
- Halcom obezbeđuje upravljanje resursima (inventar informacionih resursa, ovlašćenja i odgovornosti, razdvajanje resursa i podataka različitih korisnika);
- Informacioni sistem na bazi odluke klijenta, nadležnog državnog organa, organa lokalne samouprave ili direktno na osnovu važećih propisa garantuje efikasan način brisanja podataka o ličnosti;
- Halcom klijentu obezbeđuje siguran prenos podataka i sprečava neovlašćeni pristup podacima o ličnosti prilikom njegovog prenosa, uključujući prenos preko javnih telekomunikacionih sredstava i mreža (npr. enkripcija);
- Halcom sprečava neovlašćeni pristup podacima o ličnosti na fizičkim medijima na taj način što:
    - nosioci podataka sa podacima o ličnosti neće biti ostavljeni na otvorenim prostorima kancelarijske opreme ili na drugim mestima gde su dostupni neovlašćenim licima,
    - podaci o ličnosti za štampanje moraju biti bezbedno uklonjeni iz štampača nakon štampanja;
    - otpadni papiri i drugi nosioci podataka sa podacima o ličnosti moraju biti uništeni na način koji onemogućava čitanje svih ili delova uništenih podataka; isto treba uraditi sa pomoćnim materijalom;
    - neispravni mediji ili mediji za otpad sa podacima o ličnosti ne smeju se bacati u kante za otpatke, već se moraju bezbedno uništiti.
- i druge obaveze koje proističu iz propisa o zaštiti podataka o ličnosti, ovih opštih uslova i ugovora.

6 PODIZVOĐAČI

Član 15

(1) Halcom može angažovati podizvođače za izvršavanje ugovornih zadataka koji uključuju obradu podataka o ličnosti, pod uslovom da o tome obavesti klijenta u pisanoj formi o svakom novom podizvođaču ili o značajnoj promeni u ugovornom odnosu sa postojećim podizvođačem najmanje 30 dana pre početka zadataka, a klijent se u roku od 8 dana od dana prijema obaveštenja, ne protivi pismenim putem.

(2) Halcom može angažovati podugovarače po sopstvenom nahođenju za obavljanje poslova po ugovoru, koji ne uključuju obradu podataka o ličnosti.

(3) Halcom garantuje za zadatke koje obavljaju podizvođači, kao da ih sam izvršava.

7 UPRAVLJANJE PROMENAMA

Član 16

Promene u informacionim rešenjima ili dokumentaciji koja proizlazi iz ugovora mogu poticati od:

- razloga za poboljšanje ili uvođenje novih rešenja koja su predmet ovog ugovornog odnosa;
- uklanjanje grešaka u informacionim rešenjima koja su predmet ovog ugovornog odnosa;
- organizacionih promena koje utiču na rešenja koja su predmet ovog ugovornog odnosa ili
- zakonskih promena koje utiču na rešenja koja su predmet ovog ugovornog odnosa.

Član 17

(1) Razvojno, testno i produkciono okruženje informacionih rešenja koja su predmet ovog ugovornog odnosa su uvek potpuno odvojeni.

(2) Svaka izmena informacionih rešenja ili dokumentacije koja je predmet ovog ugovornog odnosa prvo će se testirati isključivo u razvojnom okruženju i isključivo sa imaginarnim podacima ili javno dostupnim digitalnim sadržajem. Svaka promena mora biti ispravno dokumentovana označavanjem nove verzije deskriptivnim identifikovanjem uzroka promene i suštinskog ažuriranja, i određivanjem lokacije zadržavanja nove i prethodne verzije.

(3) Sve verzije informacionog rešenja i dokumentacije se uvek čuvaju bezbedno.

(4) Realni podaci nikada ne smeju da napuste produkciono okruženje i ne mogu se preneti u bilo koje drugo okruženje ili preneti drugim osobama bez izričite osnove u merodavnom zakonu ili bez izričitog pristanka svih ugovornih partnera i krajnjeg klijenta, na koga se podaci odnose i nakon prethodne procene da li je takva aktivnost u skladu sa svim važećim propisima.

Član 18

(1) Pre instalacije nove verzije informacionog rešenja:

- predvideti metodu i moguće probleme instalacije i rada u sistemu;
- uspešno testirati novu verziju u test okruženju, koja je ispravno dokumentovana;
- u skladu sa promenama, kompletirati ili na drugi način revidirati projektnu dokumentaciju.

(2) Nove verzije informacionih rešenja, koja su predmet ovog ugovornog odnosa, ne smeju se instalirati pre nego što svi zadaci iz prethodnih stavki budu uspešno i ispravno izvršeni.

(3) Izmenjeno **infromaciono** rešenje, koje je predmet ovog ugovornog odnosa, biće instalirano nakon što se o tome jednoglasno dogovore ugovorni partneri.

Član 19

(1) Pre instaliranja novog informacionog rešenja, aplikacijsku podršku za usluge koje su predmet ovog ugovornog odnosa, ili instalaciju izmene postojećeg informacijskog rešenja, potrebne aktivnosti za obuku ili informisanje svih zaposlenih ili korisnika, određuje rukovodilac projektne grupe.

(2) Oba ugovorna partnera su obavezna da obezbede neophodne kooperativne aktivnosti tako da se zaposleni i/ili korisnici mogu adekvatno i efektivno upoznati sa novim informacionim rešenjima ili promenama.

8 NEPREKIDNO POSLOVANJE

Član 20

(1) Halcom je dužan da obezbedi važeći plan kontinuiteta poslovanja, koji ima za cilj pružanje usluga 24/7 klijentu, uspostavljanje procedura za sprečavanje prekida kontinuiteta poslovanja, garantovanje nesmetanog rada pojedinačnih usluga, plan postupaka u slučaju kvara usluge i garantovanje usklađenosti sa važećim propisima i ovog ugovornog odnosa.

(2) Plan se mora zasnivati na proceni rizika i ugovornoj proceni rizika, uz predlog mera za smanjenje tih rizika u slučaju mogućih hitnih slučajeva.

(3) Plan najmanje mora imati sledeće:

- postojanje krizne grupe koja mora preuzeti odgovornost za upravljanje u slučaju vanrednog stanja i koja preuzima glavne akcije prilikom donošenja odluka, a koje su periodični sastanci u cilju preventivnog pregleda plana kontinuiteta poslovanja i njegovog ažuriranja;
- predviđene prve korake u slučaju hitnosti i identifikaciju uzroka i posledice;
- plan komunikacije za hitne slučajeve;
- obavezno periodično testiranje plana kontinuiteta poslovanja (najmanje jednom godišnje ili pri svakoj većoj promeni u procesima, opremi ili izloženosti rizicima, obavezna pravila operativnih testova, simulacija kvara cele primarne lokacije, obnova rada na primarnoj lokaciji).

9 ZAŠTITA PODATAKA I IZVEŠTAVANJE O INCIDENTIMA

Član 21

(1) Na zahtev klijenta ili nadležnih državnih organa, Halcom će, u svakom pojedinačnom slučaju pripremiti i dostaviti izveštaje o funkcionisanju informacionog sistema pomenutog u ovom ugovornom odnosu, obradi podataka ili tehničkog lista za zaštitu zakonskih prava, u vezi sa zadacima ili podacima koje je obradio prema ugovoru.

(2) Ako nije drugačije dogovoreno, klijent je dužan da plati cenu izrade izveštaja ili ispisa iz prethodnog stava na osnovu njegovog zahteva ili zahteva nadležnog državnog organa, prema izvršenim radnim satima po važećem cenovniku.

Član 22

(1) Halcom je obavezan da prati i beleži sve događaje u vezi sa bezbednošću informacija (incidentima), tj. bilo koji događaj koji ima ili bi mogao imati kao rezultat obradu podataka o ličnosti prema ovom ugovornom odnosu:

- nedostupnost sistema ili njegovog dela ili usluga;
- otkrivanje poverljivih informacija, gubitak ili neželjena promena podataka;
- oštećenje ili gubitak opreme i sredstava ili
- druge radnje koje krše sigurnosnu politiku ili sigurnosne procedure.

(2) Halcom garantuje da ovlašćeni i stručno osposobljeni radnici reaguju na bilo koji događaj informacione bezbednosti i preuzimaju sve potrebne mere kako bi sprečili posledice događaja i sprečili buduće negativne događaje.

(3) Halcom pruža klijentu informacije o svim kritičnim događajima u vezi sa informacionom bezbednošću koji mogu imati ozbiljne posledice.

(4) Ako je potreban poseban izveštaj i nije drugačije dogovoreno, klijent je dužan da plati prijave incidenta iz prethodnih stavova na osnovu njegovog zahteva ili zahteva nadležnog državnog organa prema izvršenim radnim satima po važećem cenovniku, osim ako se incident dogodio od strane Halcoma.

10 UNUTRAŠNJA KONTROLA

Član 23

(1) Klijent ima pravo da kontroliše Halcomovu implementaciju i usklađenosti sa važećim srpskim propisima, međunarodnim standardima i preporukama i stručnim znanjem u radnjama prema ugovornom odnosu.

(2) U tom cilju, Halcom garantuje poslovanje u skladu sa ISO/IEC 27001, koji jednom godišnje verifikuje nezavisno spoljno telo za ocenjivanje usaglašenosti i, na zahtev klijenta, Halcom potvrđuje da ima važeći ISO / IEC 27001 sertifikat.

11 REGULATORNE OBAVEZE I UPRAVLJANJE UGOVOROM

Član 24

(1) Na zahtev klijenta, Halcom je dužan da osigura saradnju svojih zaposlenih i obezbedi sve potrebne dokaze za potencijalne potrebe klijenta u vezi sa procedurama za ostvarivanje prava pojedinca ili u vezi sa internim ili eksternim revizijskim postupcima ili nadzorom nadležnih državnih organa ili sudskim, arbitražnim ili srodnim postupcima.

(2) Ako nije drugačije dogovoreno, klijent je dužan da nadoknadi trošak Halcomovog učešća u nadzoru iz prethodnih članova prema izvršenim radnim satima, osim u slučaju kad se incident dogodio od strane Halcoma.

Član 25

(1) Halcom mora obavljati svoje zadatke na način koji omogućava klijentu da vrati podatke u svoju implementaciju ili drugom pružaocu. U te svrhe klijent može da zahteva od Halcoma da se dogovore o mogućnostima izvoza podataka, operativnog plana prenosa podataka i drugih povezanih mera.

(2) Po završetku pojedinačne obrade, ako je tako dogovoreno ili kada Halcom raskine ugovor, Halcom dostavlja sve podatke klijentu i rezultate obrade, a nakon potvrde uspešnog dostavljanja podataka od strane klijenta, briše ili blokira sve podatke i ne obrađuje podatke o ličnosti na druge načine.

12 KOMUNIKACIJA IZMEĐU UGOVORNIH STRANA

Član 26

(1) Sve komunikacije, zahtevi ili druga komunikacija koja se odnosi na ugovorni odnos moraju biti u pisanoj formi i dostavljeni lično ili poslati preporučenom poštom ili elektronski, putem kvalifikovanog pružaoca usluga elektronske dostave ili kvalifikovanim elektronskim potpisom, adresiranim na zvanično sedište klijenta ili adresu navedenu u poglavlju ugovora ili na adresu koju je ta strana dala.

(2) Ako datum prijema nije evidentiran, datum prijema obaveštenja ili pošiljke važi 8 dana od datuma poštanskog žiga.

13 ODGOVORNOST

Član 27

(1) U skladu sa važećim propisima Republike Srbije, Halcom je obavezan da nadoknadi štetu klijentu za svako neovlašćeno otkrivanje podataka o ličnosti ili poverljivih informacija dobijenih na osnovu ugovornog odnosa ili u svrhu postizanja dogovorene poslovne svrhe. Ako je za nastalu štetu ili oslabljenu poziciju Halcoma odgovoran korisnik, ili druga osoba za koju je korisnik odgovoran, Halcomova obaveza nadoknade štete se srazmerno smanjuje. Halcom nije odgovoran za štetu koju je u aktivnostima prema ovim opštim uslovima ili ugovornom odnosu prouzrokovao klijent.

(2) U svakom slučaju, Halcom ne preuzima nikakvu materijalnu odgovornost za indirektnu štetu nastalu nepravilnim radom Halcomovog informacionog rešenja, koje je klijent prihvatio za rad u svom proizvodnom okruženju.

(3) Halcomova obaveza nadoknade štete je ograničena, bez obzira na osnov odgovornosti za štetu, ako zakonom nije predviđeno drukčije, na iznos koji klijent Halcomu plaća za usluge u periodu od 3 meseca pre nastanka štete.

(4) U ovom slučaju klijent se mora izjasniti o nastaloj šteti ili ugovornoj kazni, a Halcom se obavezuje da će platiti odštetu ili ugovornu kaznu u roku od 15 dana od dana izdavanja računa, na osnovu obrazloženog zahteva.

(5) Smatra se da je zahtev opravdan ako je propraćen odgovarajućim dokazima iz kojih proizlazi da je Halcom prekršio odredbe ugovora ili ovih opštih uslova.

Član 28

(1) Nijedna strana neće biti odgovorna za štetu zbog kašnjenja i/ili grešaka u pružanju usluga pod ovim opštim uslovima ili ugovornim odnosima, pod uslovom da je do takvog kašnjenja ili greške došlo zbog okolnosti van kontrole bilo koje ugovorne strane u sledećim, ali ne isključivo, primerima:

- ograničenja u radu vlasti;
- rat, nemiri i drugi socijalni prevrati;
- zemljotresi, poplave ili druge prirodne katastrofe;
- drugi razlozi izvan kontrole bilo koje ugovorne strane.

(2) Ugovorna strana koja, zbog više sile, ne može u potpunosti ili delimično da ispuni obaveze iz ovih opštih uslova ili ugovornog odnosa, mora o tome obavestiti, u pisanom obliku, odmah, a najkasnije u roku od dva radna dana ugovornu stranu u slučaju nastanka više sile, i mora izneti procenu trajanja i moguće posledice više sile, kao i da dostavi dokaze o ovoj pojavi.

14 ZAVRŠNE ODREDBE

Član 29

(1) Ako je bilo koja od ugovornih odredbi nevažeća ili postane nevažeća to ne utiče na druge ugovorne odredbe. Nevažeća odredba se zamjenjuje važećom, koja mora biti što je moguće bliža svrsi koju je pokušala postići nevažeća odredba.

(2) Ako se odredbe ovih opštih uslova ne primenjuju ili ako se zahteva primena odredbi, takvo odricanje neće se tumačiti kao raskid relevantnih odredbi i neće uticati na valjanost ovih opštih uslova ili ugovornog odnosa, delimično, ili u celini ili u prestanku prava bilo koje ugovorne strane na osnovu ovih opštih uslova.

Član 30

Za sporove pod ovim opštim uslovima, prema pravu Republike Srbije **nadležan je sud u Beogradu**.

Član 31

(1) Halcom ima pravo da izmeni i dopuni ove opšte uslove, obaveštavajući klijenta elektronskim putem najmanje dva meseca pre predviđene primene izmenjenih opštih uslova.

(2) Smatraće se da klijent prihvata predlog za izmenu opštih uslova, ako Halcom ne primi pismeno obaveštenje dan pre predloženog datuma njihove važnosti, da predlog nije prihvaćen ili da je ugovor otkazan.

Član 32

Ovi opšti uslovi važe od 21. 08. 2019.

Beograd, 21.08.2019.

Aleksandar Spremić

direktor

ANEKS 1: Integrisana privatnost

1. Proaktivnost umesto reaktivnosti

Ugrađeni koncept privatnosti zasniva se na proaktivnom delovanju, kako bi se izbegli problemi, a ne reaktivnom ispravljanju. Potencijalne probleme u vezi sa zaštitom podataka o ličnosti i privatnosti treba pravovremeno predvideti, a dizajn sistema treba prilagoditi na način koji smanjuje rizik od zloupotrebe, a ne čeka na implementaciju tih rizika. Ako se ugrađeni koncept privatnosti ne uzme u obzir, a kada se takvo rešenje dizajnira i koristi, prilagođavanje rešenja će koštati vremena, resursa i ugleda. U nekim slučajevima, naknadno prilagođavanje sistema može koštati više nego da se sistem izgradi od početka.

2. Privatnost kao podrazumevani izbor

Postavke prilagođene privatnosti treba definisati kao zadate u informacionim rešenjima. Primeri takvih podešavanja mogu biti:

- polja za pristanak sa kojima se pojedinac slaže da pristaje na obradu njegovih podataka treba da po *difoltu* bude prazna – saglasnost treba dati pojedinac aktivnom radnjom;
- podešavanja dostupnosti ili javnosti podataka (na primer, na sajtovima društvenih mreža) treba da budu podešena kao podrazumevana na najviši stepen poverljivosti podataka.

3. Privatnost, koja je sastavni deo dizajna rešenja

Privatnost treba da bude ugrađena u dizajn i arhitekturu informacionih rešenja i poslovnih praksi, a ne tek naknadno. Privatnost se mora razmotriti već u fazi uspostavljanja funkcionalnih zahteva sistema, a takođe treba predvideti i naknadne metode osiguranja privatnosti tokom celog životnog ciklusa sistema.

4. Puna funkcionalnost – igra se sa pozitivnom sumom

Bitan element ugrađenog koncepta privatnosti je pružanje potpune funkcionalnosti – integracijom privatnosti ne bi trebalo da se žrtvuju performanse sistema ili drugih legitimnih ciljeva. Često čujemo da treba žrtvovati privatnost zbog veće sigurnosti, udobnosti ili ekonomičnosti, a koncept ugrađene privatnosti se zasniva na pronalaženju rešenja koja nas ne prisiljavaju da biramo, nego pružaju oboje. A to, po pravilu, zahteva znanje i vreme, ponekad i veće resurse, ali je održavanje privatnosti ono što se želi postići.

5. Bezbednost podataka tokom ciklusa obrade podataka

Zaštita podataka je važan element zaštite podataka o ličnosti i odnosi se na sprečavanje neovlašćene obrade podataka o ličnosti i slučajnih ili namernih promena ili gubitka podataka o ličnosti. Brigu o pravilnoj zaštiti podataka o ličnosti treba smatrati procesom, a ne samo individualnim zadacima koji se završavaju kada se završe. Proces zaštite podataka o ličnosti mora biti zasnovan na planiranju, implementaciji, verifikaciji i odgovoru na identifikovane nepravilnosti i nedostatke. U tom smislu, preporučuje se poštovanje smernica međunarodno utvrđenih standarda informacione bezbednosti, kao što su standardi iz porodice ISO/IEC 27000, kao i periodična verifikacija prisutnosti poznatih ranjivosti, koje mogu potpuno poništiti druge mere.

6. Transparentnost

Zatvorena rešenja koja navodno garantuju zaštitu podataka o ličnosti i koja se zasnivaju na našem poverenju, iako se ne mogu verifikovati, nisu u skladu sa konceptom ugrađene privatnosti. Nasuprot tome, rešenja za privatnost moraju omogućiti nezavisnu spoljašnju proveru i potvrdu stvarne zaštite podataka o ličnosti. Iz sveta kriptografije, na primer, postoje poznati slučajevi kada su korišćene skrivene kriptografske metode, kako bi, kao rezultat tajne, trebalo da budu bezbedne, ali nažalost, često se pokazalo da su rešenja koja su bila predmet javne diskusije ona na kojima su "slomili zube" i najbolji istraživači sa svim raspoloživim sredstvima. Prosečan programer će teško sam razviti siguran kripto algoritam, i u tom smislu, potrebno je koristiti verifikovane kriptografske metode.

7. Poštovanje pojedinca

Dizajn rešenja takođe treba da uzme u obzir aspekt pojedinca i omogući mu da bude adekvatno informisan o obradi podataka o ličnosti, podrazumevanim jednostavnim postavkama privatnosti i tako dalje. Rešenja koja prikrivaju informacije o obradi podataka o ličnosti u nečitljivim politikama privatnosti i u komplikovanim i tehnološki orijentisanim postavkama koje normalni korisnik uopšte ne razume, ne zadovoljavaju koncept ugrađene privatnosti.

Koncept ugrađene privatnosti predstavlja osnovu za izradu smernica za razvoj informatičkih rešenja, koja su detaljnije prikazana u nastavku.