SPLOŠNI POGOJI O ZAGOTAVLJANJU SKLADNOSTI GLEDE INFORMACIJSKIH REŠITEV IN INFORMACIJSKIH STORITEV

1 UVODNE DOLOČBE

1. člen

(1) Splošni pogoji družbe Halcom d.d. o zagotavljanju skladnosti glede informacijskih rešitev in informacijskih storitev (v nadaljevanju: splošni pogoji) opredeljujejo pogoje partnerskega sodelovanje ter pravice in obveznosti izvajalca oziroma dobavitelja Halcom d.d. (v nadaljevanju: Halcom ali izvajalec) in kupca ali naročnika (v nadaljevanju naročnik) v zvezi z varstvom podatkov (osebni podatki, poslovne skrivnosti), skladnostjo procesov in rešitev ter drugimi področji zagotavljanja skladnosti z veljavnimi slovenskimi in evropskimi predpisi ter mednarodnimi in evropskimi tehničnimi standardi in priporočili.
(2) Splošni pogoji imajo značaj pogodbe in so njen sestavni del, jo dopolnjujejo ter zavezujejo pogodbeni stranki enako kot pogodba. S sklenitvijo pogodbe s Halcom d.d. naročnik izjavlja, da je seznanjen z vsebino splošnih pogojev in to vsebino v celoti sprejema. Če se določila splošnih pogojev in pogodbe razlikujejo, veljajo določila pogodbe.
(3) Halcom naročniku ob podpisu pogodbe posreduje elektronski izvod splošnih pogojev. Splošni pogoji so na voljo tudi na sedežu izvajalca.

2. člen

(1) Pogodbeni stranki soglašata, da bosta skladno s predpisi o varstvu osebnih podatkov zagotavljali pogoje in ukrepe za zagotovitev varstva osebnih podatkov in preprečevali morebitne zlorabe, skladno in v smislu z določili navedenih predpisov.
(2) Halcom izjavlja, da ima registrirano dejavnost obdelovanja podatkov po splošni klasifikaciji dejavnosti oziroma drugo ustrezno dejavnost, ki jo veljavni predpisi o varstvu podatkov zahtevajo kot pogoj za opravljanje pogodbene obdelave osebnih podatkov
(3) Halcom bo pogodbeno obdeloval osebne podatke v imenu in za račun naročnika skladno s slovenskimi in evropskimi veljavnimi predpisi, mednarodnimi in evropskimi standardi ter drugimi pravili stroke, to pogodbo in navodili naročnika.

3. člen

(1) V tej prilogi je pogodbena stranka, ki razkriva določene informacije imenovana "posredovalna stranka" ter stranka, ki prejema te informacije, "prejemna stranka".
(2) "Zaupne informacije" po tej pogodbi so vse poslovne skrivnosti oziroma informacije komercialne, finančne in tehnične narave ter vse druge informacije, ki pri posredovalni stranki veljajo kot zaupne, in so pripravljene v kakršnikoli obliki vključno s programsko opremo, analizami, preglednicami, podatki, študijami ali drugimi dokumenti, ki jih pripravi prejemna stranka na podlagi oziroma v zvezi z zaupnimi informacijami. Kot zaupne informacije veljajo tudi vsi dokumenti, ki jih prejemna stranka pripravi na podlagi takih informacij ali ki vsebujejo oziroma so popolnoma ali delno pripravljeni na podlagi takih informacij.

2 POOBLASTILA ZA OBDELAVO OSEBNIH PODATKOV

4. člen

Naročnik pooblašča Halcom, da obdeluje osebne podatke skladno z določili pogodbe oziroma te priloge k pogodbi, ki je sestavni del pogodbenega razmerja.
Nabor podatkov:

a. podatki o pooblaščencih na bančnih računih ki vključujejo (osebno ime, naslov prebivališča, davčna številka, naslov elektronske pošte, telefonska številka, serijska številka avtentikacijskega sredstva in drugi podatki glede pooblaščenca, avtentikacije in pooblastil);

b. aktivnosti, sporočila in dokumenti pooblaščencev v elektronski banki (čas povezave, IP naslov, identifikacijsko sredstev, izvedene akcije in posredovana sporočila ali dokumenti v elektronski banki);
c. aktivnosti, sporočila in dokumenti banke (čas povezave, IP naslov, identifikacijsko sredstev, prejeta sporočila ali dokumenti v elektronski banki);
d. revizijske sledi (čas aktivnosti, osebno ali uporabniško ime, podatki o aktivnosti oziroma vnosu, spremembi ali dostopu do podatkov).

Namen obdelave: izvajanje plačilnih storitev in drugih storitev med naročnikom in eno ali več poslovnih bank, zagotavljanje učinkovitosti delovanja storitev in zagotavljanje informacijske varnosti ter druge naloge skladno s pogodbo.
Čas obdelave: skladno z veljavnimi predpisi - 10 let od transakcije po predpisih o preprečevanju pranja denarja in financiranja terorizma; 3 oziroma 5 let glede na obligacijski zastaralni rok od prenehanja pogodbenega razmerja med komitentom in banko, omejeno s časom trajanja pogodbenega razmerja po tej pogodbi in prilogi. Revizijske sledi se skladno s predpisi o varstvu podatkov, obligacijskim zastaralnim in kazenskim zastaralnim rokom hranijo 6 let od dneva posameznega informacijskega dogodka, ukrepa oziroma transakcije.

5. člen

(1) Halcom sme osebne podatke obdelovati izključno v obsegu in samo za namene in v obdobju, kot je določen v pooblastilu iz prejšnjega člena.
(2) Ob prenehanju veljavnosti te pogodbe ali kadarkoli na zahtevo naročnika je Halcom dolžan zagotoviti izbris ali blokiranje osebnih podatkov, ki jih je prejel ali jih obdeluje na podlagi pooblastila iz prejšnjega člena skladno z določili pogodbe.
(3) Ob prenehanju veljavnosti te pogodbe ali kadarkoli na zahtevo naročnika je Halcom dolžan naročniku izročiti vse ali del osebnih podatkov, ki jih je prejel ali jih obdeluje na podlagi pooblastila iz prejšnjega člena skladno z določili pogodbe.
(4) Obveznosti iz tega člena Halcom ne sme nikakor pogojevati in jih je dolžan izvršiti ne glede na status pogodbenega razmerja, morebitne spore z naročnikom ali morebitne neporavnane obveznosti naročnika. Halcom lahko odkolni izpolnitev obveznosti samo, če tako določa zakon ali pravni akt ali odločitev Evropske unije, ki je najmanj enakovredna zakonu.

3 POSLOVNE SKRIVNOSTI

6. člen

Vse zaupne informacije posredovalne stranke so last te stranke oziroma je nosilec pravic intelektualne lastnine, kar ji druga stranka priznava. Prejemni stranki posredovanje teh informacij ne podeljuje nobenih pravic v zvezi s posredovanimi informacijami.

7. člen

(1) Obveznosti določene s temi splošnimi pogoji se ne nanašajo na zaupne informacije, ki:

- jih prejemna stranka že poseduje še preden jih je prejela s strani posredovalne stranke;
- so ali postanejo javne iz drugega razloga, kot pa zaradi kršenja tega dogovora;
- jih je prejemna stranka neodvisno razvila;
- jih prejemna stranka na podlagi vnaprejšnjega izrecnega pisnega pooblastila posredovalne stranke lahko posreduje tretji osebi;
- so prejete s strani tretje osebe brez podobnih omejitev in brez kršenja tega dogovora;
- so posredovana s strani prejemne stranke na zahtevo pristojnega sodišča ali drugega državnega organa.

(2) V primerih posredovanja državnim organom mora prejemna stranka obvestiti nasprotno stranko pred posredovanjem teh informacij, tako da lahko posredovalna stranka sprejme vse potrebne ukrepe za ustrezno zaščito svojih pravic v zvezi z zahtevanimi zaupnimi informacijami. Prejemna stranka mora v vsakem primeru posredovati državnim organom le tisti del zaupnih informacij, za katere je zahtevano z zakonom, da se posredujejo

in se mora potruditi po svojih najboljših močeh, da bo pridobila od prejemnika informacij izjavo o varovanju poslovne skrivnosti ali drugo ustrezno zagotovilo, da se bo s posredovanimi informacijami ravnalo zaupno;
(3) Z izjemo zgoraj navedenih točk bodo obveznosti iz teh splošnih pogojev ostale v veljavi tudi po uresničitvi poslovnega namena ali prekinitvi pogodbenega razmerja iz kakršnegakoli razloga.

8. člen

(1) Stranki dogovora se strinjata, da bosta zaupne informacije razkrili in zagotovili druga drugi, v obsegu kot je potrebno za uresničitev poslovnega namena. Stranki se dogovorita, da zaupnih informacij druge stranke ne bosta posredovali tretji osebi, bodisi fizični osebi, podjetju, družbi, združenju ali kateremkoli drugemu subjektu iz kakršnegakoli razloga ali namena.
(2) Strankama je dovoljeno posredovati zaupne informacije svojim zaposlenim. Zaposlenim se smejo posredovati le tiste informacije, ki jih le-ti potrebujejo pri svojem delu.

9. člen

(1) Stranki se dogovorita, da ne bosta brez izrecnega predhodnega pisnega soglasja posredovalne stranke uporabili, izrabili ali na kakršenkoli drug način uporabili posredovanih zaupnih informacij razen za uresničevanje poslovnega namena.
(2) Prejemna stranka bo omejila dostop do zaupnih informacij svojim zaposlenim, in sicer jim bo posredovala le informacije, ki so potrebne za njihovo delo. Zaupnih informacij ne bo posredovala drugim osebam, če to ni izrecno navedeno v tem dogovoru.

10. člen

(1) Posredovalna stranka lahko kadarkoli pisno zahteva vrnitev katerekoli posredovane pisne zaupne informacije v skladu s pogoji tega dogovora in tudi vse eventualne kopije, skupaj s pisno izjavo Prejemne stranke, da le ta ni zavestno zadržala v svoji lasti ali pod svojim nadzorom - posrednim ali neposrednim kakršnekoli zaupne informacije ali kopije le-te. Prejemna stranka bo svojo obveznost vrnitve zaupnih informacij izpolnila v 8 (osmih) dneh od prejetja take zahteve.
(2) Del zaupnih informacij, ki ga sestavljajo le analize, preglednice, študije ali drugi dokumenti, pripravljeni za prejemno stranko in ki jih ta v skladu s tem dogovorom ne vrne posredovalni stranki bo na njeno zahtevo uničen, kar bo prejemna stranka pisno potrdila.

11. člen

Vsaka stranka potrjuje in jamči drugi stranki, da je ustanovljena in deluje skladno z veljavnimi predpisi v državi, v kateri je ustanovljena. Vsaka stran potrjuje, da pravno veljavno sklepa ta dogovor in da bo izvedla vse potrebne aktivnosti v zvezi z uresničevanjem tega dogovora. Posredovalna stranka jamči, da s posredovanjem zaupnih informacij ne krši nobenega drugega dogovora s tretjimi osebami.

4 VARNOST GLEDE OSEBJA

12. člen

(1) Halcom zagotavlja, da pri obdelavi osebnih podatkov sodelujejo samo njegovi zanesljivi zaposleni, ki so:

- bili primerno preverjeni v postopkih zaposlovanja ter je izpolnjevanje pogojev tudi kasneje stalno preverjano;
- pogodbeno ali s posebno izjavo zavezani k varovanju občutljivih podatkov;
- strokovno usposobljeni za svoje delo ter svoje znanje in veščine stalno ohranjajo.

(2) Halcom bo zaposlenim omogočil dostop do osebnih podatkov ali zaupnih informacij, ki je nujno potreben za njihovo delo v zvezi z nalogami po pogodbi. Prav tako bo zagotovil, da so občutljive naloge primerno urejene ter njihovo izvajanje med seboj ločeno (segregacija dolžnosti) ter se za kritične naloge zahteva sodelovanje najmanj dveh pooblaščenih in usposobljenih zaposlenih (načelo štirih oči) ter se v največji meri preprečuje, da bi posamezen zaposlen samostojno ogrozil varnost in celovitost osebnih podatkov ali zaupnih informacij.

(3) Pogodbeni stranki se dogovorita tudi, da se zaupne informacije, ne pa nujno tudi osebni podatki, lahko posredujejo tudi njihovim profesionalnim svetovalcem, agentom in svetovalcem pod pogojem da le-ti podpišejo izjavo, o varovanju zaupnosti pod enakimi pogoji, ki so vsebovani v tem dogovoru.
(4) Določbe prejšnjih odstavkov se smiselno uporabljajo tudi za zunanje sodelavce ali zaposlene podizvajalcev, če sodelovanje z njimi odobri naročnik.

5 TEHNOLOŠKA VARNOST

13. člen

(1) Pogodbeni stranki se strinjata, da bosta hranili zaupne informacije druge strani po enakih standardih varstva informacij, ki jih uporabljata za varovanje lastnih zaupnih informacij in da se bo z zaupnimi informacijami ravnalo in poslovalo na tak način, da se prepreči nepooblaščeno razkrivanje le teh.
(2) Halcom bo za izvajanje nalog po pogodbi in teh splošnih pogojih uporabljal mednarodno uveljavljeno opremo priznanih izvajalcev ali uveljavljene odprtokodne rešitve ter storitve uveljavljenih in preverjenih dobaviteljev (kakovost storitev, tehnološka usposobljenost, finančna trdnost in podobno).
(3) Halcom je dolžan imeti vzpostavljen učinkovit sistem informacijske varnosti skladno z mednarodnimi standardi (SIO 27001), kar dokazuje z rednimi neodvisnimi zunanjimi presojami in veljavnim certifikatom.
(4) Za izvajanje ključnih nalog po pogodbi ali nalog, ki lahko pomembno vplivajo na izvajanje nalog po pogodbi ali varstvo osebnih podatkov lahko Halcom uporablja podizvajalce skladno z določili 15. člena teh splošnih pogojev.
(5) Halcom je dolžan voditi popis informacijskih virov (informacijski viri, stopnja ogroženosti, varnostni ukrepi, odgovorna oseba itd.) ter ažurno dokumentacijo o izvedenih delih, nastavitvah opreme, prijavnih imenih in geslih, popisu opreme, kontaktne osebe posamezne lokacije.
(6) Vsa vzdrževalna dela morebitne strojne opreme se morajo opravljati na samem mestu, kjer se oprema nahaja. Če to ni mogoče, se mora nosilce podatkov iz opreme odstraniti in jih varno shraniti. Če podatkov ni mogoče odstraniti ali kako drugače zaščititi, mora biti postopek vzdrževanja nadzorovan. Po vzdrževalnih delih mora biti oprema, preden se jo vključi v obratovanje, varnostno pregledana.

14. člen

Halcom zagotavlja varnost in hrambo podatkov v skladu s svojimi internimi akti in varnostnimi politikami, v katerih predvidi vse potrebne organizacijske, tehnične in logično-tehnične postopke in ukrepe za zagotavljanje informacijske varnosti in varstva osebnih podatkov.
Interni akti ali varnostne politike urejajo najmanj naslednje obveznosti:

- Halcom zagotovi, da se vsi prostori, kjer se nahaja informacijski sistem ali njegovi deli oziroma varnostne kopije podatkov, ter osebni podatki na fizičnih ali elektronskih nosilcih podatkov fizično ali elektronsko varujejo;
- Halcom zagotovi fizično in elektronsko varnost strojne opreme, sistemske in aplikativne programske opreme, vključno z vhodno-izhodnimi enotami ter varnost osebnih podatkov na fizičnih ali elektronskih nosilcih zapisa v skladu z načeli informacijske varnosti;
- Halcom zagotavlja operativno varnost (elektronsko varovanje in omrežna varnost, aplikativna varnost, revizijske sledi in podobno);
- Halcom zagotavlja upravljanje identitet in dostopov (pooblastila, identitete, upravljanje ključev, šifriranje, avtentikacija, revizijske sledi);
- Halcom zagotavlja upravljanje virov (popis informacijskih virov, pooblastila in obveznosti glede upravljanja, ločenost virov ali vsaj podatkov različnih naročnikov);
- informacijski sistem na podlagi odločitve naročnika, pristojnega državnega organa,
- organa lokalne samoupravne skupnosti ali neposredno na podlagi veljavnih predpisov, zagotavlja učinkovit način izbrisa osebnih podatkov;
- skupaj z naročnikom Halcom skrbi za varen prenos podatkov in preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po javnih telekomunikacijskih sredstvih in omrežjih (npr. šifriranje);
- Halcom preprečuje nepooblaščen dostop do osebnih podatkov na fizičnih nosilcih zapisa tako, da:

- se nosilci podatkov z osebnimi podatki ne puščajo na odprtih površinah pisarniške opreme ali drugih mestih, kjer so dostopni nepooblaščenim osebam,
- osebni podatki, ki se tiskajo, se morajo po končanem tiskanju varno odstraniti iz tiskalnikov,
- odpadni papirji in drugi nosilci podatkov z osebnimi podatki se morajo uničiti na način, ki onemogoči branje vseh ali dela uničenih podatkov; enako je potrebno ravnati tudi s pomožnim materialom;
- neuničene odpadne nosilce podatkov z osebnimi podatki se ne sme odmetavati v koše za smeti, temveč jih je potrebno varno uničiti.

- ter druge obveznosti, ki izhajajo iz predpisov o varstvu osebnih podatkov in te pogodbe.

6 PODIZVAJALCI

15. člen

(1) Za izvajanje nalog po pogodbi, ki vključujejo obdelavo osebnih podatkov, lahko Halcom najema podizvajalce pod pogojem, da o vsakem novem podizvajalcu ali bistveni spremembi pogodbenega razmerja z obstoječim podizvajalcem pisno obvesti naročnika vsaj 30 dni pred začetkom izvajanja nalog ter naročnik temu v roku 8 dni od prejema obvestila pisno ne nasprotuje.
(2) Za izvajanje nalog po pogodbi, ki ne vključujejo obdelave osebnih podatkov, lahko Halcom najame podizvajalce po lastni presoji.
(3) Za naloge, ki jih opravljajo podizvajalci, Halcom jamči, kot bi jih opravljal sam.

7 UPRAVLJANJE SPREMEMB

16. člen

Spremembe informacijskih rešitev ali dokumentacije, ki nastopijo po pogodbi, lahko izvirajo iz:
- razlogov za izboljšavo ali uvedbo novih rešitev, ki so predmet te pogodbe,
- odprave napak na informacijskih rešitvah, ki so predmet te pogodbe,
- organizacijskih sprememb, ki vplivajo na rešitve, ki so predmet te pogodbe ali
- pravnih sprememb, ki vplivajo na rešitve, ki so predmet te pogodbe.

17. člen

(1) Razvojno, preizkusno in produkcijsko okolje informacijskih rešitev, ki so predmet te pogodbe, so vedno popolnoma ločeni.
(2) Vsaka sprememba informacijskih rešitev ali dokumentacije, ki so predmet te pogodbe, se najprej preizkuša izključno v razvojnem okolju in izključno z imaginarnimi podatki ali javno dostopnimi digitalnimi vsebinami. Vsaka sprememba se mora ustrezno dokumentirati, in sicer tako, da se označi nova različica, opisno opredelijo vzroki spremembe in bistvene dopolnitve ter določi mesto hrambe nove in prejšnje različice.
(3) Vedno se varno hranijo vse različice informacijske rešitve in dokumentacije za nazaj.
(4) Realni podatki ne smejo nikoli zapustiti produkcijskega okolja in se ne smejo prenašati v nobeno drugo okolje ali posredovati drugim osebam brez izrecne podlage v veljavnem zakonu ali brez izrecnega soglasja vseh pogodbenih partnerjev in končne stranke, na katero se podatki nanašajo, ter po vnaprejšnji presoji, ali je takšno ravnanje v skladu z vsemi veljavnimi predpisi.

18. člen

(1) Pred vsakokratno namestitvijo nove različice informacijske rešitve se:
- predvidi način in morebitni problemi namestitve in delovanja v sistemu,
- uspešno preizkusi nova različica v testnem okolju, kar se ustrezno dokumentira,
- skladno s spremembami dopolni oziroma drugače popravi projektna dokumentacija.

(2) Novih različic informacijskih rešitev, ki so predmet te pogodbe, ni dopustno nameščati, preden se uspešno in pravilno izvedejo vsa opravila po prejšnjem odstavku.
(3) Spremenjena informacijska rešitev, ki je predmet te pogodbe, se namesti potem, ko se pogodbena partnerja o tem soglasno dogovorita.

19. člen

(1) Pred namestitvijo nove informacijske rešitve oz. aplikativne podpore za storitve, ki so predmet te pogodbe, oziroma namestitvijo spremembe že obstoječe informacijske rešitve vodja projektne skupine določi potrebne aktivnosti za usposabljanje oziroma informiranje vseh sodelavcev oziroma uporabnikov.
(2) Oba pogodbena partnerja sta dolžna zagotoviti potrebne sodelovalne aktivnosti, da se lahko sodelavce oziroma uporabnike ustrezno in učinkovito seznani z novimi informacijskimi rešitvami oziroma spremembami le-teh.

8 NEPREKINJENO POSLOVANJE

20. člen

(1) Halcom je dolžan zagotavljati veljaven načrt neprekinjenega poslovanja, katerega namen je zagotavljati 24/7 delovanje storitev za naročnika, določiti postopke za preprečevanje prekinitve poslovne dejavnosti neprekinjenega poslovanja, zagotoviti nemoteno poslovanje posameznih storitev, opisati postopke v primeru izpada storitve in zagotoviti skladnost z veljavnimi predpisi in to pogodbo.
(2) Načrt mora temeljiti na izdelani oceni tveganja in obveznosti po pogodbi s predlogom ukrepov za zmanjšanje teh tveganj v primeru možnih izrednih dogodkov.
(3) Načrt mora vsebovati najmanj naslednje vsebine:

- obstoj krizne skupine, mora prevzeti upravljanje v primeru izrednega dogodka in sprejemati glavne odločitve ukrepanja ter ki se periodično sestanke z namenom preventivnega pregleda načrta neprekinjenega poslovanja in njegovega ažuriranja;
- predvidene prve korake v primeru izrednega dogodka in ugotavljanje vzroka in posledic;
- komunikacijski načrt za primere izrednih dogodkov;
- obvezno periodično preizkušanje načrta neprekinjenega poslovanja (vsaj enkrat letno oziroma ob vsaki večji spremembi procesov, opreme ali izpostavljenosti tveganjem; obvezna operativna pravila preizkušanja; simulacija izpada celotne primarne lokacije; obnovitev delovanja na primarni lokaciji).

9 ZAGOTAVLJANJE PODATKOV IN POROČANJE INCIDENTOV

21. člen

(1) Halcom bo na zahtevo naročnika ali pristojnih državnih organov v zvezi z nalogami ali podatki, ki jih obdeluje po pogodbi, vsakokrat v razumnem času pripravljal in posredoval poročila o delovanju informacijskega sistema iz te pogodbe, obdelavi podatkov ali izpise podatkov za varstvo pravnih upravičenj naročnika ali tretjih oseb.
(2) Če ni drugače dogovorjeno, je naročnik je dolžan plačati ceno priprave poročil ali izpisov iz prejšnjega odstavka na podlagi svoje zahteve ali zahteve pristojnega državnega organa po opravljenih človek/urah.

22. člen

(1) Halcom je dolžan spremljati in evidentirati vsak informacijski varnostni dogodek (incidente), torej vsak dogodek, ki ima ali bi lahko glede obdelav osebnih podatkov po tej pogodbi imel za posledico:

- nerazpoložljivost sistema ali njegovega dela oziroma storitev,
- razkritje zaupnih podatkov ali izgubo oz. nezaželeno spremembo podatkov,
- poškodovanje ali izgubo opreme in sredstev, ali
- drugo dejanje, ki krši varnostno politiko ali varnostne postopke.

(2) Halcom zagotavlja, da se pooblaščeni in strokovno usposobljeni zaposleni odzovejo na vsak informacijski varnostni dogodek ter izvedejo vse potrebne ukrepe za preprečevanje posledic dogodka in za preprečevanje bodočih takšnih dogodkov.
(3) Halcom naročniku zagotavlja podatke o vseh kritičnih informacijsko varnostnih dogodkih, ki imajo lahko hujše posledice.
(4) Če se zahteva posebno poročilo in ni drugače dogovorjeno, je naročnik je dolžan plačati ceno poročanja incidenta iz prejšnjih odstavkov na podlagi svoje zahteve ali zahteve pristojnega državnega organa po opravljenih človek/urah, razen v primeru, če je do incidenta prišlo zaradi razlogov na strani Halcom.

10 NOTRANJI NADZOR

23. člen

(1) Naročnik ima pravico nadzora Halcom nad izvajanjem oziroma spoštovanjem veljavnih evropskih in slovenskih predpisov, mednarodnih standardov in priporočil ter dognanj stroke pri izvajanju te pogodbe.
(2) Halcom v ta namen zagotavlja poslovanje skladno s standardom ISO/IEC 27001, kar enkrat letno preverja neodvisna zunanja presoja in Halcom na zahtevo naročnika dokazuje z veljavnim certifikatom ISO/IEC 27001.

11 REGULATORNE OBVEZNOSTI IN UPRAVLJANJE POGODBE

24. člen

(1) Halcom je dolžan na zahtevo naročnika temu zagotoviti sodelovanje svojih zaposlenih ter zagotoviti vsa potrebna dokazila za morebitne potrebe naročnika v zvezi s postopki za uveljavljanje pravic posameznika ali v zvezi s postopki notranjih ali zunanjih revizij ali nadzora s strani pristojnih državnih organov oziroma sodnih, arbitražnih ali sorodnih postopkov.
(2) Če ni drugače dogovorjeno, je naročnik dolžan plačati ceno sodelovanja Halcom pri nadzoru iz prejšnjih členov po opravljenih človek/urah, razen v primeru, če je do incidenta prišlo zaradi razlogov na strani Halcom.

25. člen

(1) Halcom mora svoje naloge izvajati na način, ki naročniku omogoča prenosljivost podatkov nazaj v lastno izvajanje ali k drugemu izvajalcu. V ta namen lahko naročnik zahteva, da delovna skupina naročnika in Halcom dogovori možnosti izvoza podatkov, operativni načrt predaje podatkov in druge sorodne ukrepe.
(2) Po končani posamezni obdelavi, če je tako dogovorjeno, ali ob prekinitvi pogodbe Halcom naročniku preda vse podatke rezultate in rezultate obdelav ter po potrditvi uspešne predaje podatkov s strani naročnika vse podatke izbriše ali blokira in ne obdeluje osebnih podatkov na druge načine.

12 SPOROČILA MED STRANKAMA

26. člen

(1) Vsa sporočila, zahteve ali druga komunikacija, ki se nanaša na pogodbeno razmerje mora biti v pisni obliki in se jo izroča osebno, ali se pošilja priporočeno s povratnico ali v elektronski obliki preko ponudnika storitev zaupanja ali s kvalificiranim elektronskim podpisom vročitve, naslovljeno na stranko ali stranke na uradni ali naslov naveden v glavi pogodbe ali na naslov, ki ga sporoči ta stranka.
(2) Če datum prejema ni evidentiran, kot datum prejetja obvestila ali pošiljke velja 8 dan po datumu poštnega žiga.

13 ODŠKODNINSKA ODGOVORNOST

27. člen

(1) Halcom skladno z veljavnimi predpisi Republike Slovenije odškodninsko odgovarja naročniku za vsako nepooblaščeno razkritje osebnih podatkov ali zaupnih informacij pridobljenih na podlagi pogodbenega razmerja oziroma zaradi uresničitve dogovorjenega poslovnega namena. Če je za nastalo škodo ali otežitev položaja Halcoma kriv tudi naročnik oziroma druga oseba, za katero je odgovoren naročnik, se Halcomova odškodninska sorazmerno zmanjša. Halcom ne odgovarja za škodo, ki je pri izpolnjevanju teh splošnih pogojev oziroma pogodbenega razmerja povzročena s strani naročnika.
(2) Halcom v nobenem primeru ne prevzema nobene materialne odgovornosti za posredno škodo, ki bi bila posledica nepravilnega delovanja Halcomove informacijske rešitve, ki je s strani naročnika sprejeta v delovanje v njegovem produkcijskem okolju.
(3) Odškodninska odgovornost Halcoma je, ne glede na temelja odškodninske odgovornosti, po višini omejena na znesek, ki ga je naročnik plačala Halcomu za storitve v obdobju 3 mesecev pred nastankom škodnega dogodka.
(4) Naročnik v tem primeri izstavi obračun nastale škode ali pogodbene kazni, izvajalec pa se obvezuje, da bo nastalo škodo ali pogodbeno kazen plačal v roku 15 dni od izstavitve obračuna na podlagi utemeljene zahteve.

(5) Šteje se, da je zahteva utemeljena, če so ji priloženi ustrezni dokazi, iz katerih izhaja, da je izvajalec kršila določbe pogodbe ali teh splošnih pogojev.

28. člen

(1) Nobena od pogodbenih strank ni odgovorna za škodo zaradi zamud in/ali napak pri izvajanju storitev iz teh splošnih pogojev ali pogodbenega razmerja, če je takšna zamuda oziroma napaka nastala zaradi okoliščin, na katere ni mogla vplivati nobena od pogodbenih strank, vključujoč predvsem, vendar ne izključno, naslednje primere:

- omejitev in ukrepov oblastnih organov,
- vojne, nemirov in drugih socialnih prevratov,
- potresov, poplav ali drugih naravnih ujm in katastrof,
- drugih razlogov, na katere ni mogla vplivati nobena od pogodbenih strank.

(2) Pogodbena stranka, ki zaradi nastopa višje sile delno ali v celoti ne more izpolnjevati obveznosti po teh splošnih pogojev oziroma pogodbenem razmerju, mora takoj, najkasneje pa v dveh delovnih dneh od dneva, ko je izvedela za višjo silo, v pisni obliki obvestiti nasprotno stranko o nastopu višje sile, predvidenem trajanju in morebitnih posledicah višje sile ter ji posredovati dokazila o njenem nastanku.

14 KONČNE DOLOČBE

29. člen

(1) Če katera koli od pogodbenih določb je ali postane neveljavna, to ne vpliva na ostale pogodbene določbe. Neveljavna določba se nadomesti z veljavno, ki mora čimbolj ustrezati namenu, ki ga je želela doseči neveljavna določba.
(2) Če določila teh splošnih pogojev niso izvajana ali če se ne zahteva izvajanje določil, se takšna opustitev zahteve ne tolmači kot prenehanje veljavnosti ustreznih določil ter ne vpliva na veljavnost teh splošnih pogojev oziroma pogodbenega razmerja, niti deloma, niti v celoti ali na prenehanje pravic katerekoli pogodbene stranke na podlagi teh splošnih pogojev.

30. člen

Za spore po teh splošnih pogojih je pristojno sodišče v Ljubljani po pravu Republike Slovenije.

31. člen

(1) Naročnik ima pravico spremeniti ali dopolniti te splošne pogoje, o čemer bo izvajalca po elektronski poti obvestil najmanj dva meseca pred predvidenim začetkom uporabe spremenjenih splošnih pogojev.
(2) Šteje se, da izvajalec sprejema predlog sprememb splošnih pogojev, če do dneva pred predlaganim datumom začetka njihove uporabe naročnik ne prejme njegovega pisnega obvestila, da predloga ne sprejema ali da od pogodbe odstopa.

32. člen

Ti splošni pogoji veljajo od 03.01.2018 dalje.

Ljubljana, 03.01.2018

Marko Valjavec
Glavni direktor

halcom® d.d. Ljubljana

PRILOGA 1: Vgrajena zasebnost

1. Proaktivnost namesto reaktivnosti

Koncept vgrajene zasebnost temelji na proaktivnem delovanju, na izogibanju težavam namesto reaktivnega odpravljanja posledic. Potencialne težave z vidika varstva osebnih podatkov in zasebnosti naj bi pravočasno predvideli in dizajn sistema vnaprej prilagodili na način, ki zmanjšuje tveganja za zlorabe namesto čakanja na udejanjenje teh tveganj. Če koncept vgrajene zasebnosti ne bo upoštevan in ko bo enkrat takšna rešitev oblikovana in v uporabi, vas bo prilagajanje rešitve stalo časa, sredstev in ugleda, v nekaterih primerih pa vas lahko naknadno popravljanje sistema stane več, kot če bi sistem porušili in postavili na novo.

2. Zasebnost kot privzeta izbira

Zasebnosti prijazne nastavitve naj bi bile v informacijskih rešitve opredeljene kot privzete (angl. default). Primeri takšnih nastavitev so lahko:

- potrditvena polja, s katerimi posameznik potrdi strinjanje z obdelavo svojih podatkov naj bodo privzeto prazna – strinjanje naj posameznik z izpolnitvijo aktivno poda;
- nastavitve javnosti podatkov (npr. na spletnih družbenih omrežjih) naj bodo privzeto nastavljene na zaupnost podatkov.

3. Zasebnost, ki je sestavni del zasnove rešitve

Zasebnost naj bi bila vgrajena v samo zasnovo in arhitekturo informacijskih rešitev in poslovnih praks, ne pa naknadno dodana. Zasebnost mora biti obravnavana že v fazi postavljanja funkcionalnih zahtev sistema, prav tako pa morajo biti predvideni naknadni načini zagotavljanja zasebnosti v celotnem življenjskem ciklu sistema.

4. Polna funkcionalnost - igra s pozitivno vsoto

Bistven element koncepta vgrajene zasebnosti je zagotavljanje polne funkcionalnosti – z vgradnjo zasebnosti ne bi smeli žrtvovati učinkovitosti delovanja sistema ali drugih legitimno zasledovanih ciljev. Pogosto slišimo, da moramo žrtvovati zasebnost zaradi višje varnosti, praktičnosti ali ekonomičnosti, koncept vgrajene zasebnosti pa temelji na iskanju rešitev, ki nas ne silijo v izbiranje med navedenimi, temveč zagotavljajo oboje. In da, to praviloma terja znanje in čas, včasih tudi višja sredstva, toda prav tako praviloma se da ohraniti zasebnost in kljub temu doseči zasledovane cilje.

5. Zavarovanje podatkov v celotnem ciklu obdelave podatkov

Zavarovanje podatkov je pomemben element varstva osebnih podatkov in se nanaša na preprečevanje nepooblaščene obdelave osebnih podatkov ter slučajne ali namerne spremembe ali izgube osebnih podatkov. Skrb za ustrezno zavarovanje osebnih podatkov moramo obravnavati kot proces in ne le kot posamezne naloge, ki so končane, ko so enkrat opravljene. Proces zavarovanja osebnih podatkov mora temeljiti na načrtovanju, izvajanju, preverjanju in reagiranju na odkrite nepravilnosti in pomanjkljivosti. Pooblaščenec v tem oziru vsem upravljavcem osebnih podatkov priporoča upoštevanje smernic mednarodno uveljavljenih standardov varovanja informacij, kot so standardi iz družine standardov ISO/IEC 27000, kakor tudi periodično preverjanje prisotnosti znanih ranljivosti, ki lahko popolnoma izničijo ostale ukrepe.

6. Transparentnost

Zaprte rešitve, ki domnevno zagotavljajo varstvo osebnih podatkov in ki temeljijo na našem zaupanju vanje, kljub

temu, da jih ni mogoče preveriti, niso v skladu s konceptom vgrajene zasebnosti. In obratno, rešitve z vgrajeno zasebnostjo morajo omogočati neodvisen zunanji pregled in potrditev dejanskega varovanja osebnih podatkov. Iz sveta kriptografije so na primer znani primeri, ko so bile uporabljene skrite kriptografske metode, ki naj bi bile zaradi te tajnosti tudi varne, a se je žal večkrat pokazalo, da so res varne le tiste rešitve, ki so bile povržene javni presoji in na katerih so si »zobe polomili« tudi najboljši raziskovalci z vsemi razpoložljivimi sredstvi. Povprečen razvijalec bo le stežka zapisal varen kripto algoritem, zato se je v tem oziru treba držati preverjenih kriptografskih metod.

Javnost seveda sama po sebi še ni zagotovilo, da bo neka rešitev varnostno neoporečna, a bi javna presoja morala biti v določenih primerih nujna – takšen primer je recimo uvajanje bodočih pametnih osebnih izkaznic.

7. Spoštovanje posameznika

Dizajn rešitev bi moral upoštevati tudi vidik posameznika in mu omogočiti ustrezno informiranost glede obdelave osebnih podatkov, privzete enostavno uporabne nastavitve zasebnosti in podobno. Rešitve, ki informacije o obdelavi osebnih podatkov zakrivajo v neberljivih politikah zasebnosti in v kompliciranih in preveč tehnološko usmerjenih nastavitvah, ki jih običajni uporabnik sploh ne razume, ne zadostijo konceptu vgrajene zasebnosti.

Koncept vgrajene zasebnosti predstavlja osnovo za smernice za razvoj informacijskih rešitev, ki jih v nadaljevanju podrobneje predstavljamo.

Vir in več informacija: Smernice za razvoj informacijskih rešitev (Informacijski pooblaščenec RS)