POLITIKA VAROVANJA OSEBNIH PODATKOV

Kazalo vsebine

1. Namen, področje uporabe in uporabniki

BIOTOPIC d.o.o., Cvetlična ulica 9, 3000 Celje, v nadaljnjem besedilu "Družba" oz. **Biotopic**, si prizadeva izpolniti veljavne zakone in predpise v zvezi z varstvom osebnih podatkov v državah, v katerih družba posluje. Ta pravilnik (oziroma politika ali dokument varovanja osebnih podatkov) določa temeljna načela, s katerimi podjetje obdeluje osebne podatke potrošnikov, kupcev, dobaviteljev, poslovnih partnerjev, zaposlenih in drugih posameznikov ter opozarja na odgovornosti svojih poslovnih oddelkov in zaposlenih pri obdelavi osebnih podatkov.

Pravilnik velja za družbo in njene neposredno ali posredno nadzorovane hčerinske družbe v popolni lasti, ki poslujejo v Evropskem gospodarskem prostoru (EGP), ali za obdelavo osebnih podatkov posameznikov, na katere se podatki nanašajo, v EGP.

Uporabniki tega dokumenta so vsi zaposleni, stalni ali začasni, in vsi izvajalci, ki delajo v imenu družbe.

2. Referenčni dokumenti

- EU GDPR 2016/679 (Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varovanju fizičnih oseb v zvezi z obdelavo osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46 / ES)
- Zakon o varovanju osebnih podatkov (ZVOP-2)
- Zakon o varstvu potrošnikov (ZVPot)
- Politika varovanja informacij
- Politika hrambe podatkov

3. Definicije

Naslednje opredelitve pojmov, uporabljenih v tem dokumentu, izhajajo iz člena 4 Splošne uredbe Evropske unije o varstvu podatkov:

Osebni podatki: vse informacije o določeni ali določljivi fizični osebi ("oseba s podatki"), ki se lahko neposredno ali posredno identificira, zlasti glede na identifikator, kot so ime, identifikacijska številka, podatki o lokaciji, spletni identifikator ali na enega ali več dejavnikov, značilnih za fizično, fiziološko, gensko, duševno, gospodarsko, kulturno ali družbeno identiteto te fizične osebe.

Občutljivi osebni podatki: osebni podatki, ki so po svoji naravi posebej občutljivi glede na temeljne pravice in svoboščine, zaslužijo posebno varstvo, saj bi kontekst njihove obdelave lahko povzročil znatno tveganje za temeljne pravice in svoboščine. Ti osebni podatki vključujejo osebne podatke, ki razkrivajo rasno ali etnično poreklo, politična prepričanja, verska ali filozofska prepričanja ali članstvo sindikatov, genetske podatke, biometrične podatke z namenom enolične identifikacije fizične osebe, podatki o zdravju ali podatki o spolu fizične osebe življenje ali spolno usmerjenost.

Upravljalec podatkov (nadzornik ali kontrolor podatkov): fizična ali pravna oseba, javni organ, agencija ali kateri koli drug organ, ki sam ali skupaj z drugimi določa namene in sredstva za obdelavo osebnih podatkov.

Obdelovalec podatkov (procesor podatkov): fizična ali pravna oseba, javni organ, agencija ali kateri koli drug organ, ki obdeluje osebne podatke v imenu upravljalca podatkov.

Obdelava: Operacija ali niz operacij, ki se izvajajo na osebnih podatkih ali na skupinah osebnih podatkov, ne glede na to, ali z avtomatskimi sredstvi, kot so zbiranje, beleženje, organizacija, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, iskanje, razkritje s prenosom, razširjanje ali dostopnost na drug način , usklajevanje ali kombiniranje, omejevanje, brisanje ali uničevanje podatkov.

Anonimizacija: nepopravljivo odkrivanje osebnih podatkov, tako, da oseb ni mogoče identificirati z uporabo razumnega časa, stroškov in tehnologije, bodisi s strani upravljalca ali katere koli druge osebe, da identificira to osebo. Načela obdelave osebnih podatkov se ne uporabljajo za anonimne podatke, saj niso več osebni podatki.

Psevdonimizacija: obdelava osebnih podatkov na tak način, da osebnih podatkov ni več mogoče pripisati določenemu posamezniku, na katerega se podatki nanašajo, brez uporabe dodatnih informacij, pod pogojem, da se take dodatne informacije vodijo ločeno in so predmet tehničnih in organizacijskih ukrepov, s katerimi se zagotovi, da se osebni podatki ne pripisujejo določeni ali določljivi fizični osebi. Psevdonimizacija zmanjšuje, vendar ne popolnoma odpravlja, možnost povezovanja osebnih podatkov s posameznikom, na katerega se podatki nanašajo. Ker so psevdonimizirani podatki še vedno osebni podatki, mora biti obdelava psevdonimiranih podatkov v skladu z načeli obdelave osebnih podatkov.

Kontaktna oseba za zaščito podatkov (DPC, Data Protection Contact):

- je prva kontaktna točka za vsa vprašanja o varstvu podatkov v podjetju,
- nadzoruje varovanje operativnih podatkov,
- izvaja notranje svetovanje in ocenjuje pomisleke,
- usklajuje izmenjavo podatkov,
- spremlja skladnost z zakonskimi predpisi o varstvu podatkov v podjetju,
- svetuje in podpira tehnična vprašanja,
- je kontakt za varstvo podatkov sv posamezni družbi, ki opravlja posebne naloge varstva podatkov na kraju samem,
- vprašanja in naloge glede varstva podatkov so osredotočena na DPC in se z DPC uredijo in usklajujejo.

Čezmejna obdelava osebnih podatkov: Obdelava osebnih podatkov, ki potekajo v okviru dejavnosti ustanov v več kot eni državi članici upravljavca ali obdelovalca v Evropski uniji, kjer ima upravljavec ali obdelovalec sedež v več kot eni državi članici; ali obdelavo osebnih podatkov, ki poteka v okviru dejavnosti ene same ustanove upravljavca ali obdelovalca v Evropski Uniji, vendar bistveno prizadene

ali bi lahko bistveno vplivala na posameznike, na katere se podatki nanašajo, v več kot eni državi članici.

Nadzorni organ: neodvisen javni organ, ki ga država članica ustanovi v skladu s členom 51 BDP EU;

Vodilni nadzorni organ: nadzorni organ, pristojen za obravnavanje dejavnosti čezmejne obdelave podatkov, na primer, ko posameznik, na katerega se podatki nanašajo, vloži pritožbo pri obdelavi njegovih osebnih podatkov; je med drugim odgovoren za prejemanje obvestil o kršitvi podatkov, ki jih je treba priglasiti v zvezi s tvegano predelovalno dejavnostjo, in bo imela polno pooblastilo v zvezi z njegovimi dolžnostmi za zagotavljanje skladnosti z določbami BDP EU;

Vsak "lokalni nadzorni organ" bo še vedno nadziral in spremljal vsako lokalno obdelavo podatkov, ki vpliva na posameznike, na katere se podatki nanašajo, ali ki jih izvaja upravljalec ali obdelovalec v EU ali izven EU, kadar je obdelava namenjena osebam s podatki, ki prebivajo na njenem ozemlju . Njihove naloge in pooblastila vključujejo izvajanje preiskav in uporabo upravnih ukrepov in glob, spodbujanje ozaveščenosti javnosti o tveganjih, pravilih, varnosti in pravicah v zvezi z obdelavo osebnih podatkov ter dostop do vseh prostorov upravljavca in obdelovalca , vključno z opremo in sredstvi za obdelavo podatkov.

"Glavna poslovna enota oz. sedež upravljavca", s poslovnimi enotami ali podjetji v več kot eni državi članici, je kraj njegove osrednje uprave v EU, razen če se odločitve o namenih in sredstvih za obdelavo osebnih podatkov sprejmejo v drugi enoti upravljavca v EU in je slednja pooblaščena za izvajanje takih odločitev, pri čemer se ustanova, ki je sprejela take odločitve, šteje za glavno poslovno enoto;

" Glavna poslovna enota oz. sedež obdelovalca" s poslovnimi enotami ali podjetji v več kot eni državi članici EU, je kraj njegove osrednje uprave v EU ali, če predelovalec nima centralne uprave v EU, ustanovitev obdelovalca v EU, kjer glavne obdelovalne dejavnosti v okviru dejavnosti obratov obdelovalca potekajo v obsegu, za katerega veljajo posebne obveznosti v skladu s to uredbo;

Skupina: vsake podjetje holdinga skupaj s hčerinsko družbo.

4. Osnovna načela v zvezi z obdelavo osebnih podatkov

Načela varstva podatkov opisujejo osnovne odgovornosti organizacij, ki ravnajo z osebnimi podatki. Člen 5 (2) BDP določa, da "je upravljavec odgovoren in sposoben dokazati skladnost z načeli."

4.1. Zakonitost, poštenost in preglednost

Osebne podatke je treba obdelati zakonito, pošteno in pregledno glede na posameznika, na katerega se podatki nanašajo.

4.2. Omejitev namena

Osebne podatke je treba zbirati za določene, eksplicitne in zakonite namene in se ne smejo več obdelovati na način, ki ni združljiv s temi nameni.

4.3. Minimizacija podatkov

Osebni podatki morajo biti ustrezni, ustrezni in omejeni na tisto, kar je potrebno glede na namene, za katere se obdelujejo. Družba mora anonimizirati ali psevdonimizirati osebne podatke, če je mogoče, da zmanjša tveganja za zadevne osebe, na katere se podatki nanašajo.

4.4. Ohranjevanje natančnosti

Osebni podatki morajo biti točni in po potrebi posodobljeni; je treba sprejeti primerne ukrepe za zagotovitev, da se osebni podatki, ki so netočni, ob upoštevanju namenov, za katere se obdelujejo, pravočasno izbrišejo ali popravijo.

4.5. Omejitev časa shranjevanja

Osebne podatke je treba hraniti največ, kot je potrebno za namene, za katere se obdelujejo osebni podatki.

4.6. Celovitost in zaupnost

Ob upoštevanju stanja tehnologije in drugih razpoložljivih varnostnih ukrepov, stroškov izvajanja ter verjetnosti in resnosti tveganj za osebne podatke mora družba uporabiti ustrezne tehnične ali organizacijske ukrepe za obdelavo osebnih podatkov na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z zaščito pred naključnim ali nezakonitim uničenjem, izgubo, izmenjavo, nepooblaščenim dostopom do ali razkritjem.

4.7. Odgovornost

Upravljavci podatkov morajo biti odgovorni in morajo biti sposobni dokazati skladnost z zgoraj navedenimi načeli.

5. Varstvo podatkov v poslovnih dejavnostih

Za dokazovanje skladnosti z načeli varstva podatkov mora organizacija varovati varstvo podatkov v svoje poslovne dejavnosti.

5.1. Obveščanje o predmetih podatkov

Oglejte si razdelek Smernice za pošteno obdelavo.

5.2. Izbira in privolitev lastnika podatkov

Oglejte si razdelek Smernice za pošteno obdelavo.

5.3. Zbirka

Družba si mora prizadevati za zbiranje najmanjšega možnega števila osebnih podatkov. Če se osebni podatki zbirajo pri tretji osebi, mora **Kontaktna oseba za zaščito podatkov (DPC, Data Protection Contact)** zagotoviti, da se osebni podatki zbirajo zakonito.

5.4. Uporaba, zadrževanje in odstranjevanje

Namen, metode, omejitev shranjevanja in obdobje hranjenja osebnih podatkov morajo biti v skladu z informacijami iz obvestila o zasebnosti. Družba mora ohranjati natančnost, celovitost, zaupnost in pomembnost osebnih podatkov na podlagi namena obdelave. Ustrezne varnostne mehanizme, namenjene varstvu osebnih podatkov, je treba uporabiti za preprečevanje kraje osebnih podatkov, zlorabo ali zlorabo ter preprečevanje kršitev osebnih podatkov. **DPC** je odgovoren za izpolnjevanje zahtev, navedenih v tem poglavju.

5.5. Razkritje tretjim osebam

Kadarkoli družba uporablja tretjega dobavitelja ali poslovnega partnerja za obdelavo osebnih podatkov v njegovem imenu, mora **DPC** zagotoviti, da bo ta obdelovalec zagotovil varnostne ukrepe za varovanje osebnih podatkov, ki so primerni za s tem povezana tveganja. V ta namen je treba uporabiti vprašalnik o skladnosti BDP-jev za obdelovalce in varnostno politiko dobavitelja.

Družba mora pogodbeno zahtevati, da dobavitelj ali poslovni partner zagotovi enako raven varstva podatkov. Dobavitelj ali poslovni partner mora obdelati osebne podatke le za izpolnjevanje svojih pogodbenih obveznosti do družbe ali po navodilih družbe in ne za druge namene. Kadar Družba obdeluje osebne podatke skupaj z neodvisno tretjo osebo, mora družba izrecno navesti svoje odgovornosti in tretjo osebo v ustrezni pogodbi ali katerem koli drugem pravno zavezujočem dokumentu, kot je Sporazum o obdelavi podatkov o dobavitelju.

5.6. Čezmejni prenos osebnih podatkov

Pred prenosom osebnih podatkov iz Evropskega gospodarskega prostora (EGP) je treba uporabiti ustrezne zaščitne ukrepe, vključno s podpisom sporazuma o prenosu podatkov, kot to zahteva Evropska unija, in če je potrebno, pridobiti dovoljenje pristojnega organa za varstvo podatkov. Subjekt, ki prejme osebne podatke, mora biti v skladu z načeli obdelave osebnih podatkov, določenimi v postopku prenosa čezmejnih podatkov.

5.7. Pravice do dostopa do podatkovnih subjektov

Kadar deluje kot upravljavec podatkov, je **DPC** odgovoren, da posameznikom, na katere se podatki nanašajo, imajo razumen dostopni mehanizem, ki jim omogoča dostop do svojih osebnih podatkov in jim mora omogočiti, da posodobijo, popravijo, izbrišejo ali pošljejo svoje osebne podatke, če je to primerno ali zahtevano z zakonom. Mehanizem dostopa bo podrobneje opisan v postopku zahtev za dostop do podatkovnih baz podatkov.

5.8. Prenos podatkov

Podatki, ki so nam jih posredovali subjekti podatkov v strukturirani obliki imajo pravico, da na zahtevo prejmejo kopijo podatkov in jih brezplačno prenesejo drugemu obdelovalcu. **DPC** je odgovoren za zagotovitev, da se takšne zahteve obdelajo v enem mesecu, niso pretirane in ne vplivajo na pravice do osebnih podatkov drugih posameznikov.

5.9. Pravica do pozabe

Subjekti podatkov imajo pravico zahtevati od družbe izbris svojih osebnih podatkov. Kadar družba deluje kot upravlajlec, mora **DPC** sprejeti potrebne ukrepe (vključno s tehničnimi ukrepi), da obvesti tretje osebe, ki uporabljajo ali obdelujejo te podatke za izpolnjevanje zahtev.

6. Navodila za pošteno obdelavo

Osebne podatke je treba obdelati le, če jih izrecno odobri **DPC**.

Družba se mora odločiti, ali bo za vsako dejavnost obdelave podatkov izvedla oceno učinka za varstvo podatkov v skladu s Smernicami za presojo vplivov na varstvo podatkov.

6.1. Obvestila o predmetih podatkov

Ob zbiranju ali pred zbiranjem osebnih podatkov za katero koli vrsto obdelave, vključno s prodajo izdelkov, storitev ali trženjskih dejavnosti, je **DPC** odgovoren za pravilno obveščanje oseb, na katere se nanašajo osebni podatki, o naslednjih vrstah:

- **vrste osebnih podatkov, ki so zbrani,**
- **namen obdelave,**
- **metode obdelave,**
- **pravice posameznikov, glede na njihove osebne podatke, na katere se nanašajo osebni podatki,**
- **obdobje hrambe,**
- **morebitne mednarodne prenose podatkov, če bodo podatki deljeni s tretjimi osebami in**
- **varnostnimi ukrepi družbe za zaščito osebnih podatkov.**

Te informacije so na voljo v obvestilu o zasebnosti.

Kadar se osebni podatki delijo s tretjimi osebami, mora **DPC** zagotoviti, da so posamezniki, na katere se podatki nanašajo, obveščeni o tem preko obvestila o zasebnosti.

Kadar se osebni podatki prenašajo v tretjo državo v skladu s politiko prenosa čezmejnih podatkov, mora obvestilo o zasebnosti to odsevati in jasno navesti, kje in kateri osebni podatki se prenašajo.

Kadar se zbirajo občutljivi osebni podatki, mora **DPC**, da Obvestilo o zasebnosti izrecno določa namen, za katerega se zbirajo občutljivi osebni podatki.

6.2. Pridobivanje soglasij

Kadar obdelava osebnih podatkov temelji na soglasju posameznika ali drugih zakonitih razlogov, je **DPC** odgovoren za vodenje evidence o takšnem soglasju. **DPC** je odgovoren za to, da posameznikom, na katere se osebni podatki nanašajo, omogoči možnost za pridobitev soglasja in jih o tem obvesti ter zagotovi, da se njihova privolitev, kadar je soglasje uporabljeno kot zakonita podlaga za obdelavo, kadarkoli prekliče.

Če se zbiranje osebnih podatkov nanaša na otroka, mlajšega od 16 let, mora **DPC** zagotoviti, da je starševsko soglasje dano pred zbiranjem s pomočjo obrazca starševskega soglasja.

Ko zahtevajo popravljanje, spreminjanje ali uničenje osebnih podatkov, mora **DPC** zagotoviti, da se te zahteve obravnavajo v razumnem časovnem okviru. **DPC** mora tudi beležiti zahtevke in voditi dnevnik teh.

Osebne podatke je treba obdelati le za namen, za katerega so bili prvotno zbrani. V primeru, da želi družba obdelati zbrane osebne podatke za drug namen, mora podjetje pridobiti soglasje svojih v jasnem in jedrnatem obrazcu. Vsaka takšna zahteva mora vključevati prvotni namen, za katerega so bili zbrani podatki in tudi novi ali dodatni namen. V zahtevek mora biti naveden tudi razlog za spremembo namena. **DPC** je odgovorna za upoštevanje pravil iz tega odstavka.

Zdaj in v prihodnje mora **DPC** zagotoviti, da so metode zbiranja skladne z ustreznimi zakoni, dobrimi praksami in industrijskimi standardi.

DPC je odgovoren za izdelavo in vzdrževanje **registra obvestil o zasebnosti**.

7. Organizacija in odgovornosti

Odgovornost za zagotavljanje ustrezne obdelave osebnih podatkov ima vsak, ki dela za družbo ali z njim in ima dostop do osebnih podatkov, ki jih obdeluje družba.

Ključna področja odgovornosti za obdelavo osebnih podatkov so naslednje organizacijske vloge:

- Uprava, upravni odbor ali drug ustrezen organ odločanja sprejema odločitve o splošnih strategijah družbe o varstvu osebnih podatkov in jih sprejema.
- **Odgovorna oseba za varovanje osebnih podatkov** (DPC) ali kateri koli drug ustrezen delavec je odgovoren za upravljanje programa za varstvo osebnih podatkov in je odgovoren za razvoj in promocijo politike varstva osebnih podatkov,
- Oddelek oz. svetovalec za pravne zadeve, skupaj z **DPC** spremlja in analizira zakone o osebnih podatkih in spremembe predpisov, razvija zahteve glede skladnosti in pomaga poslovnim oddelkom pri doseganju njihovih ciljev za osebne podatke.

Vodja IT je odgovoren za:

- Zagotavljanje vseh sistemov, storitev in opreme, ki se uporabljajo za shranjevanje podatkov, izpolnjujejo sprejemljive varnostne standarde.
- Opravljanje rednih pregledov in pregledov za zagotovitev varnosti strojne in programske opreme deluje pravilno.

Vodja trženja je odgovoren za:

- Odobritev vseh izjav o varstvu podatkov, priloženih komunikacijam, kot so e-poštna sporočila in črke.
- Obravnava morebitnih podatkovnih poizvedb novinarjev ali medijev, kot so časopisi.
- Po potrebi sodeluje z **DPC**, da zagotovi trženjske pobude, ki spoštujejo načela varstva podatkov.

Upravitelj človeških virov je odgovoren za:

- Izboljšanje ozaveščenosti vseh zaposlenih o varstvu osebnih podatkov uporabnikov.
- Organiziranje strokovnega znanja in izkušenj na področju varstva osebnih podatkov ter usposabljanja za ozaveščanje zaposlenih, ki delajo z osebnimi podatki.
- Varnost osebnih podatkov zaposlenih od začetka do konca. Zagotoviti je treba, da se osebni podatki zaposlenih obdelujejo na podlagi legitimnih poslovnih razlogov in potrebe delodajalca.

Vodja nabave je odgovoren za posredovanje odgovornosti dobaviteljem o varstvu osebnih podatkov ter za izboljšanje ozaveščenosti dobaviteljev o varstvu osebnih podatkov in za prenos zahtev po osebnih podatkih tretjim osebam, ki jih uporablja. Oddelek za naročila mora zagotoviti, da si družba pridržuje pravico do revizije dobaviteljev.

8. Smernice za ustanovitev vodilnega nadzornega organa

8.1. Nujnost ustanovitve vodilnega nadzornega organa

Določitev vodilnega nadzornega organa je pomembna samo, če družba opravlja čezmejno obdelavo osebnih podatkov. Prekrivanje osebnih podatkov se izvaja, če:

a) obdelavo osebnih podatkov izvajajo hčerinske družbe družbe, ki imajo sedež v drugih državah članicah; ali

b) obdelava osebnih podatkov, ki potekajo v eni sami ustanovi podjetja v Evropski uniji, vendar bistveno prizadene ali bi lahko bistveno vplivala na posameznike, na katere se podatki nanašajo, v več kot eni državi članici.

Če ima družba le enote v eni državi članici in njene aktivnosti obdelave vplivajo le na posameznike, na katere se podatki nanašajo, v tej državi članici, kot ni potrebe po ustanovitvi vodilnega nadzornega organa. Edini pristojni organ bo nadzorni organ v državi, kjer je družba zakonito ustanovljena.

8.2. Glavna ustanova in vodilni nadzorni organ

8.2.1. Glavna ustanova za upravljalca podatkov

Uprava družbe mora določiti glavni sedež, tako, da se lahko določi vodilni nadzorni organ.

Če ima družba sedež v državi članici EU in sprejema odločitve v zvezi s čezmejnimi dejavnostmi obdelave v kraju svoje osrednje uprave, bo za dejavnosti obdelave podatkov, ki jih izvaja družba, obstajal enoten nadzorni organ.

Če ima družba več obratov, ki delujejo samostojno in sprejemajo odločitve o namenih in sredstvih obdelave osebnih podatkov, mora Uprava družbe potrditi, da obstaja več vodilnih nadzornih organov.

8.2.2. Vzpostavitev centralne enote obdelovalca podatkov

Če družba deluje kot obdelovalec podatkov, bo centralna poslovna enota pomenila centralno administracijo. V primeru, da se mesto centralne uprave ne nahaja v EU, bo pomenila centralna poslovna enota tista, ki je v EU in kjer potekajo centralne predelovalne dejavnosti.

8.2.3. Glavna ustanova za podjetja zunaj EU za upravljalce in obdelovalce podatkov

Če družba nima glavnega sedeža v EU in ima subsidiarne člane v EU, je pristojni nadzorni organ lokalni nadzorni organ.

Če družba nima glavnega sedeža v EU in hčerinskih družb v EU, mora imenovati zastopnika v EU in pristojni nadzorni organ bo lokalni nadzorni organ, kjer se nahaja zastopnik.

9. Odziv na incidente pri kršitvah osebnih podatkov

Ko se družba seznani s sumom ali dejansko kršitvijo osebnih podatkov, mora **DPC** opraviti notranjo preiskavo in pravočasno sprejeti ustrezne sanacijske ukrepe. Če obstaja tveganje za pravice in svoboščine posameznikov, na katere se podatki nanašajo, mora družba brez nepotrebnega odlašanja in, če je mogoče, v 72 urah obvestiti pristojne organe za varstvo podatkov.

10. Revizija in odgovornost

Revizijski oddelek ali drugi ustrezni oddelek je odgovoren za revizijo, kakor tudi, kako oddelki implementirajo politico varovanja osebnih podatkov.

Vsak zaposleni, ki krši to politiko, bo predmet disciplinskega ukrepa, delavec pa je lahko predmet civilnih ali kazenskih obveznosti, če njegovo vedenje krši zakone ali predpise.

11. Konflikti prava

Ta pravilnik je namenjen izpolnjevanju zakonov in predpisov v kraju ustanovitve in držav, v katerih deluje Družba. V primeru kakršnega koli nasprotja med to politiko in veljavnimi zakoni in predpisi, prevladajo slednji.

12. Vodenje evidenc na podlagi tega dokumenta

Ime zapisa	Lokacija hrambe	Zadolžena oseba za hrambo	Ukrepi za zaščito zapisov	Čas hranjenja
Register obvestil o zasebnosti	Intranet	Kontaktna oseba za zaščito podatkov (DPC, Data Protection Contact)	Samo avtorizirane osebe lahko dostopajo do imenika	Stalno
Obrazci za soglasje in umik soglasij	Intranet	Kontaktna oseba za zaščito podatkov (DPC, Data Protection Contact)	Samo avtorizirane osebe lahko dostopajo do imenika	20 let
Pogodbe ponudnikov obdelave podatkov	Intranet	Kontaktna oseba za zaščito podatkov (DPC, Data Protection Contact)	Samo avtorizirane osebe lahko dostopajo do imenika	20 let
Urnik hranjenja podatkov	Intranet	Kontaktna oseba za zaščito podatkov (DPC, Data Protection Contact)	Samo avtorizirane osebe lahko dostopajo do imenika	20 let
Register aktivnosti obdelave	Intranet	Kontaktna oseba za zaščito podatkov (DPC,	Samo avtorizirane osebe lahko dostopajo do imenika	20 let

		Data Protection Contact)		
DPIA register	Intranet	Kontaktna oseba za zaščito podatkov (DPC, Data Protection Contact)	Samo avtorizirane osebe lahko dostopajo do imenika	20 let
Register kršitev	Intranet	Kontaktna oseba za zaščito podatkov (DPC, Data Protection Contact)	Samo avtorizirane osebe lahko dostopajo do imenika	20 let

Evidence so na voljo na spletni strani pod področjem Dokumenti in obrazci, če so javni, ali gelde na individualno zahtevo na sedežu družbe.

13. Veljavnost in upravljanje dokumentov

Ta dokument velja od 2.5.2018.

Lastnik tega dokumenta je Kontaktna oseba za zaščito podatkov (DPC, Data Protection Contact), ki mora preveriti in po potrebi posodobiti dokument vsaj enkrat letno.

Kontaktna oseba za zaščito podatkov (DPC, Data Protection Contact): Klara Titan, info@biotopic.si

_____

[podpis]

Šifra:	04.2
Verzija:	1.0
Datum verzije:	2.5.2018
Izdelal:	Družba
Potrdil:	Direktor

Stopnja zaupnosti:	Visoka

Zgodovina sprememb

Datum	Verzija	Izdelal	Opis sprememb
2.5.2018	1.0	Družba	Izdelava dokumenta