1 Tiivistelmä Varman tietoturvapolitiikasta

Varman tietoturvapolitiikka kuvaa tietoturvallisuuden merkitystä Varmalle, toteutettavan tietoturvallisuuden roolit ja vastuut sekä keskeiset tietoturvariskien hallintakeinot. Politiikan tavoitteena on osaltaan varmistaa, että Varman tiedot/Varman hallussa olevat on suojattu ja palvelut toimivat sekä normaali- että poikkeusoloissa. Politiikka koskee kaikkia Varman työntekijöitä sekä niitä sidosryhmien edustajia, jotka käsittelevät Varman tietoja. Politiikka kattaa kaikki Varman tiedot ja tietojenkäsittelyn koko niiden elinkaaren ajan. Varman johtoryhmä on hyväksynyt tietoturvapolitiikan ja vastaa siitä, että resursointi on riittävä ja sitä noudatetaan Varman toiminnassa.

1.1 Tietoturvallisuuden merkitys ja tavoitteet

Varmassa toteutettavan tietoturvallisuuden tarkoituksena on tukea Varman perustehtävää eli eläkkeiden turvaamista. Tietoturvallisuuden tavoitteet on johdettu Varman arvoista ja operatiivista tavoitteista.

Tavoitteet ovat:

- Vastuullisuus: Tietoturvatyö on vastuullista ja Varman arvoihin sekä lakisääteiseen tehtävään perustuvaa.
- Eläkepalvelujen ja sijoitustoiminnan laatu: Tietoturvallisuus on osa luotettavien ja laadukkaiden eläke- ja vakuutuspalveluiden, asiakkuuksien, sijoitustoiminnan sekä kumppanuuksien kehittämistä ja tuottamista.
- Tehokkuus: Tietoturvallisuutta toteutetaan tehokkaasti suhteessa tietoturvallisuudella hallittaviin riskeihin.

Jokainen Varman työtekijä tai Varman toimeksiannosta työskentelevä on velvollinen noudattamaan tietoturvapolitiikkaa, -periaatteita ja -ohjeita sekä huolehtimaan lainsäädännössä kulloinkin asetettujen tietoturva-, tietosuoja- ja salassapitovelvoitteiden noudattamisesta. Tästä huolehdimme jatkuvalla koulutuksella ja osaamisen varmistamisella.

1.2 Tietosuojaperiaatteet

Varman tietosuojaperiaatteissa kuvataan Varman henkilötietojen käsittelyn perusperiaatteet ja tietosuojan merkitys Varman toiminnassa. Periaatteiden tavoitteena on varmistaa, että Varmassa noudatetaan yksityisyyden suojaa ja henkilötietojen käsittelyä koskevaa lainsäädäntöä. Tietosuojaperiaatteiden pohjana on EU:n tietosuoja-asetuksen tietosuojaperiaatteet ja rekisteröidyn oikeudet. Periaatteet kattavat koko henkilötietojen elinkaaren.

Periaatteiden perustana on riskiperusteinen lähestymistapa tietosuojaan. Toisin sanoen Varma toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että henkilötietojen käsittelyssä noudatetaan EU:n tietosuoja-asetusta ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit.

1.3 Henkilötietojen käsittely Varmassa

1. Henkilötietoja käsitellään vain lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (laillisuus, kohtuullisuus ja läpinäkyvyys)
2. Henkilötietoja käsitellään vain tiettyä, nimettyä ja laillista tarkoitusta varten ja sama koskee jatkokäsittelyä (käyttötarkoitussidonnaisuus)

3. Henkilötiedot ovat asianmukaisia ja olennaisia ja käsittely rajoittuu siihen, mikä on tarpeellista suhteessa käsittelyn tarkoitukseen (tietojen minimointi)
4. Henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä, ja Varma toteuttaa kaikki kohtuulliset toimenpiteet, joilla epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä (täsmällisyys)
5. Henkilötietoja säilytetään muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen lainsäädännön ja tietojen käsittelyn tarkoituksen toteuttamista varten (säilytyksen rajoittaminen)
6. Henkilötietoja käsitellään tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus ml. suojaaminen luvattomalta tai lainvastaiselta käytöltä (Eheys ja luottamuksellisuus).

Tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyn vaiheissa. Varman on myös voitava osoittaa, että ao. velvoitteita on noudatettu.

Varma käyttää teknisiä ja organisatorisia toimenpiteitä käsittelytoimintojen suunnittelun alkuvaiheessa, jotta yksityisyys- ja tietosuojaperiaatteita suojellaan alusta saakka ('sisäänrakennettu tietosuoja'). Varma lisäksi oletusarvoisesti varmistaa, että henkilötiedot käsitellään voimassa olevien tietosuojasäännösten mukaisesti korkea yksityisyydensuoja varmistaen (esimerkiksi vain välttämättömiä tietoja olisi käsiteltävä, lyhyt säilytysaika, rajoitettu pääsy) ja etteivät henkilötiedot ole oletusarvoisesti rajoittamattomien henkilöiden käytettävissä ('oletusarvoinen tietosuoja').