

Helsingin Messukeskus 15. – 16.5.2012

Terveydenhuollon Atk-päivät

SESSIO 8.
Tietoturvallista terveydenhuoltoa

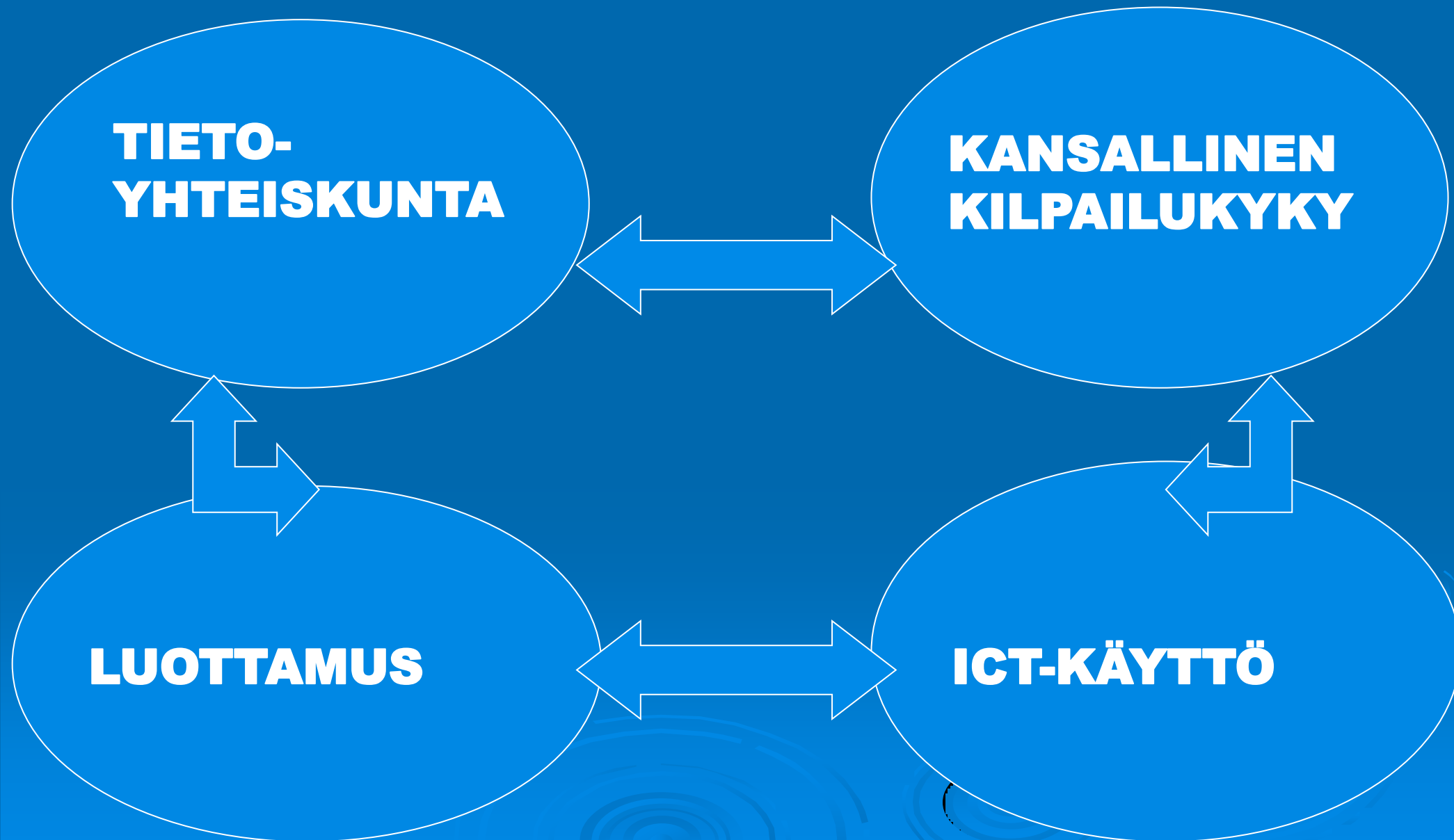
**Kansalaisten luottamus
tietoturvaan ja tietosuojaan**

Reijo Aarnio
tietosuoja-valtuutettu



**TIETOSUOJAVALTUUTETUN
TOIMISTO**

"LUOTI" -projekti



EUROBAROMETRI 2008

Rekisterinpitäjien näkemykset

- miten hyvin rekisterinpitäjät tuntevat tietosuojalainsäädännön

Hyvin

FI = 2 % (alhaisin!)

EU = 13 %

Melko hyvin

FI = 48 %

EU = 56 %

Huonosti

FI = 50 %

EU = 30 %



4. Alhaisin
(FR, PT, BE)

FI = 50 %

EU = 69 %



EU:N PERUSOIKEUSKIRJA – LISSABONIN SOPIMUS

II LUKU: VAPAUDET

7 artikla

Yksityis- ja perhe-elämän kunnioittaminen

Jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan.

8 artikla

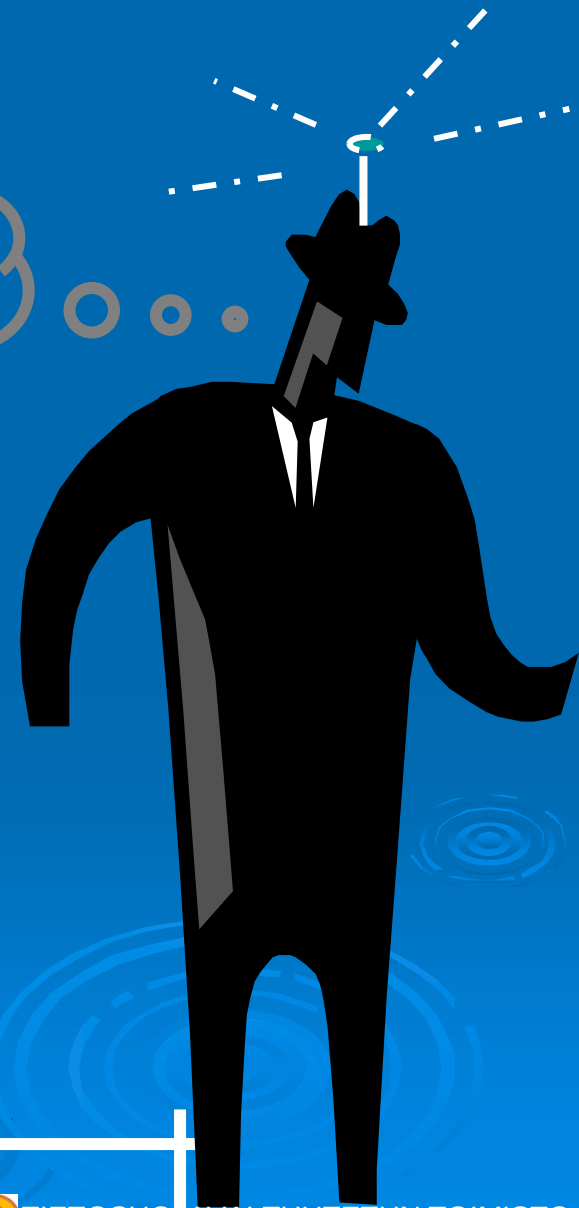
Henkilötietojen suoja

- 1.** Jokaisella on oikeus henkilötietojensa suojaan.
- 2.** Tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi.
- 3.** Riippumaton viranomainen valvoo näiden sääntöjen noudattamista.



PERUSKYSYMYS ”juridinen kiista”

**PIDÄ HAUSKAA
POIKIEN KANSSA,
KULTA!**



TIETOSUOJADIREKTIIVI 95/46/EY

Resitaalin 2) -kohta:

“Tietojenkäsittelyjärjestelmät on tehty palvelemaan ihmistä; järjestelmiä käytettäessä on kunnioitettava yksilöiden perusoikeuksia ja –vapauksia heidän kansalaisuudestaan tai asuinpaikastaan riippumatta, erityisesti oikeutta yksityisyyteen, ja osallistuttava taloudelliseen ja sosiaaliseen kehitykseen, kaupan kehittämiseen sekä yksilöiden hyvinvoinnin lisäämiseen.”



Trendit:

MUUTOSPAINETA:

- 1) Globalisaatio
- 2) Uusi teknologia
- 3) EU-parlamentin vahvistunut rooli
- 4) TI:n ratkaisut (kts. I vs Suomi)
- 5) Soveltamisalakysymykset EU-USA
- 6) Harmonisointitarve
- 7) Tietoturvalaki
- 8) Identiteettivarkaudet
- 9) Geneettiset tiedot arkaluonteisiksi tiedoiksi ?

”uudistuva tietosuoja”

Mikä:

TIETOSUOJADIREKTIIVI 95/46/EY KUMOTAAN JA KORVATAAN:

1. NEUVOSTON ASETUKSELLA
2. III-PILARIN DIREKTIIVILLÄ

Milloin:

1. KOMISSIO ANTOI ESITYKSENSÄ 25.1.2012
2. KÄSITTELYAIKA-ARVIO 12-24 KK
3. VOIMAAN HETI + 2 V SIIRTYMÄAIKA

Miksi:

1. HARMONISOINNIN PARANTAMINEN, DIGITAALISEN TALOUDEN EDISTÄMINEN
2. TEKNOLOGIAN JA UUSIEN PALVELUIDEN HAASTEET
3. HALLINNOLLISEN TAAKAN KEVENTÄMINEN
4. TIETOJEN LIKKUVUUDEN EDISTÄMINEN



”uudistuva tietosuoja”

Mitä:

1. NYKYISET PERIAATTEET SÄILYVÄT



”uudistuva tietosuoja”

Mitä:

2. ”UUSIA” ASIOITA:

- COMPLIANCE
- ACCOUNTABILITY ▶ TIETOTILINPÄÄTÖS
- PRIVACY BY DESIGN
- PRIVACY BY DEFAULT
- DATA BREACH NOTIFICATION
 - * EU KOM (2010) 245 ”A DIGITAL AGENDA FOR EUROPE”
- VALVONTAVIRANOMAISTEN ROOLIN VAHVISTAMINEN, VIRANOMAISTEN TOIMIVALTA MUUTTUU ▶
YHDENMUKAISUUSMENETTELY,
HALLINNOLLISET SANKTIOT
(JOHTAVA VALVONTAVIRANOMAINEN,
”ONE STOP SHOP”)
- EUROOPAN TIETOSUOJANEUVOSTO



”uudistuva tietosuoja”

Mitä:

2. ”UUSIA” ASIOITA (jatk.)

- TIETOTURVALAKI?
- IDENTITEETTIVARKAUKSIEN KRIMINALISOINTI?
- RIGHT TO BE FORGOTTEN
- RIGHT TO DATA PORTABILITY
- IT-JÄRJESTELMIEN AUKTORISOINTI
- KOMISSION ROOLI KASVAA
- HALLINNOLLISEN TAAKAN KEVENTÄMINEN
- TIETOSUOJAVASTAAVAT PAKOLLISIKSI



”PRIVACY BY DEFAULT”

- **vastuu ”mökin mummolta”
palvelun toimittajalle**



"PRIVACY BY DESIGN"

Henkilötietolaki (523/1999)

6 § Henkilötietojen käsittelyn suunnittelu

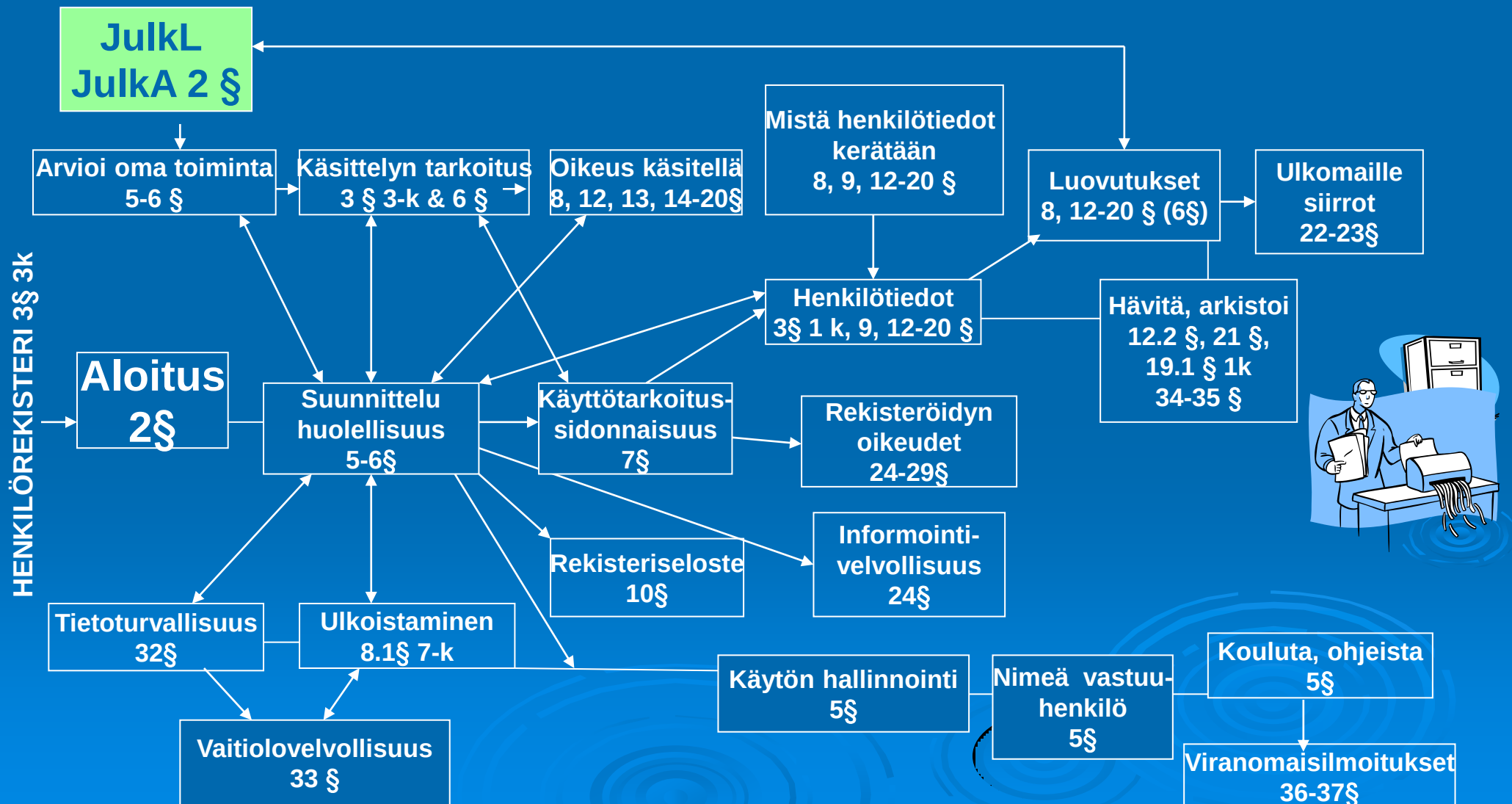
Henkilötietojen käsittelyn tulee olla asiallisesti perusteltua rekisterinpitäjän toiminnan kannalta. Henkilötietojen käsittelyn tarkoitukset sekä se, mistä henkilötiedot säännönmukaisesti hankitaan ja mihin niitä säännönmukaisesti luovutetaan, on määriteltävä ennen henkilötietojen keräämistä tai muodostamista henkilörekisteriksi. Henkilötietojen käsittelyn tarkoitus tulee määritellä siten, että siitä ilmenee, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään.



"PRIVACY BY DESIGN"

HENKILÖTIETOLAKI

Rekisterinpitäjän (3 § 4 k) henkilötietojen käsittelyn kuvaus ja lainmukaisuuden arviointi



TIETOTURVALOUKKAUKSISTA ILMOITTAMINEN

- DATA BREACH NOTIFICATION
- USA ESIMERKKINÄ
- GARTNER :
 - 1) hallitustason asiakksi
 - 2) sama salasana 10:een eri palveluun



Toimintasuunnitelma tietosuojaloukkauksen tapahduttua?

1. Havainnointi (BREACH / EVENT)
2. Käynnistys (MOBILIZE)
3. Vakauttaminen (STABILIZE)
4. Tutkinta (INVESTIGATE)
5. Tiedotus (COMMUNICATE)
6. Lievennys (MITIGATE)
7. Tiedoksianto (NOTIFY)
8. "Ota opiksi ja muuta" (REVIEW & IMPROVE)



ACCOUNTABILITY

- WP29; LAUSUNTO 3/2010
TILIVELVOLLISUUDEN PERIAATTEESTA
(13.7.2010)

”passiivisesta” compliancesta
”aktiiviseksi” accountabilityksi

- (i) soveltuvia ja tehokkaita toimia tietosuoja-periaatteiden toteuttamiseksi
- (ii) soveltuvien ja tehokkaiden toimien toteuttaminen on (pyynnöstä) todistettava

TOIMENPITEET; esimerkkejä

- 1) Sisäisen tarkastuksen menetelmät (jo ennakolta)
- 2) Ohjeistukset, "policyt" & valvonta
- 3) Tietojen kartoitus
- 4) Tietosuojaavastaavan nimeäminen
- 5) Koulutus
- 6) Valitusten ja oikeuksien käytön mekanismit
- 7) Tietoturvailmoitukset
- 8) PIA
- 9) Standardit ja sertifikaatit
- 10) Edellä mainittujen valvonta → **KUKA VALVOO?**



Tietosuojaviranomaisten suorittama lainvalvonta



TOIMIVALLAT ?



”Tietosuojatimantti”

Tietosuojavastaavat

**Data Protection
by design
(HetiL 5§)**



Tietoturva

Tietotilinpäätös

ACCOUNTABILITY



KIITOS KUUNTELUSTA!

**Tiedon laatu
= Toiminnan laatu**



**LISÄTIETOJA:
www.tietosuoja.fi**

**Reijo Aarnio
tietosuojavaaltuutettu**



Tietosuojavaaltuutetun toimisto