ANDMEKAITSE INSPEKTSIOON
Valvame, et isikuandmete kasutamisel austatakse eraelu ning et riigi tegevus oleks läbipaistev

INFOVARA BILANSS

Enesehindamise abivahend organisatsioonidele

Sissejuhatus 3
1. Mis on infovara bilanss? 4
2. Miks koostada infovara bilanssi? 4
2.1. Infovara bilanss kui usalduse looja 5
2.2. Infovara bilanss kui juhtkonna töövahend 6
2.3. Infovara bilanss kui välis- ja sisekontrolli abivahend 6
3. Infovara bilansi koostamine 6
3.1. Infovara bilansi andmed 7
3.2. Organisatsiooni valduses olevad andmekogumid 7
3.3. Andmetöötlusele kohalduvad põhimõtted ja kord 8
3.4. Infoturve 8
3.5. Andmetöötluse kontroll ja järelevalve 8
3.6. Andmesubjekti õiguste tagamine 9
4. Hindamine ja arendamist vajavad valdkonnad 9

Sissejuhatus

Majandusaasta aruannetel on organisatsioonide (avaliku sektori asutused, äriühingud, mittetulundusühingud, sihtasutused, avalik-õiguslik juriidilised isikud) majandustegevuse juhtimisel pikk ajalugu. Samalaadseid aruandeid on hakatud kasutama ka organisatsioonide tegevuse muude erinevate valdkondade korraldamisel. Majandusaasta aastaaruannet täiendavad näiteks tegevusaruanded; börsiettevõtetel ühingujuhtimise aruanded. Avalikus sektoris on kohustus auditeerida ISKE ehk infosüsteemide kolmeastmelise etalonturbe süsteemi rakendamist, sh andmekogusid.

Infovara bilansi eesmärk on kirjeldada organisatsiooni andmetöötluse hetkeseisu ja hinnata selle vastavust andmekaitse nõuetele, samuti selgitada andmetöötlusega seotud arenguvajadusi ja kavandada selleks vajalikke meetmeid.

Infovara bilanss on suunatud organisatsioonidele, kellele ei laiene otseselt seadusest tulenevad nõuded infosüsteemide, teabejuhtimise, andmetöötluse ja andmekaitse olukorra hindamiseks ning auditeerimiseks; samuti neile, kes infoturbe standardite alusel oma infovarasid muul moel regulaarselt ei inventeeri.

Organisatsiooni enesehindamise abivahendi sihtgrupiks on juhid, infoturbejuhid, IT-juhid, samuti IT-valdkonna audiitorid. Lisaks võimaldab infovara bilanss kokkuvõtlikku analüüsi, mille organisatsioonid saavad oma usaldusväärsuse kinnitamiseks avaldada koostööpartneritele ja klientidele.

Infovara bilanssi kui organisatsioonide sisehindamise ja usaldusväärsuse abivahendit kasutatakse edukalt Soomes. Parimate praktikate ülevõtmiseks Andmekaitse Inspektsioon eestindas ja kohandas Soome andmekaitsevoliniku vastava dokumendi.

1. Mis on infovara bilanss?

Infovara bilanss võib täiendada seadusjärgset majandusaasta aruandlust, kuid selle eesmärk ei ole halduskoormust asjatult tõsta. Dünaamilise töövahendina aitab see organisatsiooni tegevust tõhustada ja konkurentsivõimet parandada.

Infovara bilansi sisu võib sõltuvalt organisatsiooni tegevusalast ja tegevuse iseloomust olla erinev. See on teabejuhtimise üks osa, mida võib kasutada nii organisatsioonisisese kui ka -välise teabejuhtimise aruandena, teavitamaks erinevaid osapooli andmetöötlusega seotud põhilistest asjaoludest. Infovara bilanss on sisehindamisel põhinev aruanne, mis näiteks:

- annab ülevaate organisatsiooni andmetöötluse olukorrast;
- kirjeldab, millised andmekogumid organisatsiooni valduses on;
- kirjeldab organisatsiooni tegevusega seotud andmevooge;
- kirjeldab organisatsiooni andmevoogude ja andmetöötluse koostalitlusvõimet;
- kirjeldab, kuidas on organisatsiooni tegevuses rakendatud andmekaitse meetmeid;
- kirjeldab, kuidas on lahendatud andmetöötlusega seotud riskijuhtimine;
- on abiks plaanimises, aruandluses ja juhtimises;
- aitab hinnata arendusmeetmeid;
- on organisatsioonivälistele pooltele suunatud aruandluse vahend;
- tagab kohaldatavate õigusaktide täitmise.

Mitmed infovara bilansis käsitletavad asjaolud tulenevad isikuandmete kaitse seaduse (IKS) põhimõtetest (nt eesmärgikohasus, minimaalsus ja turvalisus). Infovara bilansi koostamine võimaldab organisatsioonil näidata, et ta järgib seadusi ja head andmetöötlustava. Infovara bilansiga seonduv dokumenteerimine paneb asju süsteemsemalt läbi vaatama ja kriitilisema pilguga hindama.

2. Miks koostada infovara bilanssi?

Info on väärtuslik ja jõudsalt kasvav tegur. Andmete kvaliteet ja tõhusad andmetöötlusreeglid mõjutavad positiivselt organisatsiooni kõiki tegevusvaldkondi. Erinevate andmekogumite ümber tekib pidevalt uusi teenuseid, mis on olulised infoühiskonna edukaks toimimiseks.

Interneti- ja infoühiskonnas on andmetöötlusel tähtis roll isikute ja organisatsioonide õiguste tagamisel ning kohustuste täitmisel. Näiteks Euroopa Inimõiguste Kohus on oma otsuses nr 20511/03 leidnud, et inimõiguste ja põhivabaduste kaitse konventsioon sobib ka infosüsteemide mõjude hindamiseks. Avaliku sektori puhul on infoturve ja andmekaitse muutunud hea haldustava püsivaks osaks. Andmetöötlus mõjutab oluliselt konkurentsivõimet, mõjukust ja organisatsioonide tõhusust.

Uued teenused ja elektroonilised protsessid eeldavad infosüsteemide ja andmetöötlusega seotud tegevuste arendamist, samal ajal tuleb leida lahendus, kuidas koos sellega tagada andmete turvaline ja vastutustundlik kasutamine. Näiteks arvutipargi ja vastavate teenuste ostmine ja kasutamine erinevate pilveteenuste vahendusel. Tänapäeval on andmekogumite haldamise tervikliku ülevaate järele selge vajadus, mida rahuldab infovara bilansi koostamine.

Infovara bilanss kirjeldab isikuandmete kaitse seaduse ja teiste heade andmetöötlustavade järgimist. Hea andmetöötlustava eeldab, et tagatud on töödeldavate andmete kättesaadavus, kaitse ja kvaliteet. Infovara bilansi koostamise tulemusena valmiv ülevaade toob kasu ka organisatsioonidele, mille tegevus põhineb suurte andmekogumite käitlemisel ja andmetöötlejate omavahelisel koostööl.

IKS § 6 kohaselt on hea andmetöötlustava põhimõtted:

- seaduslikkuse põhimõte;
- eesmärgikohasuse põhimõte;
- minimaalsuse põhimõte;
- kasutuse piiramise põhimõte;
- andmete kvaliteedi põhimõte;
- turvalisuse põhimõte;
- individuaalse osaluse põhimõte.

IKS § 24 sätestab nõuded isikuandmete töötlemisele.

IKS § 25 sisaldab sätteid isikuandmete organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete kohta.

IKS § 26 sätestab isikuandmeid töötlevatele isikutele esitatavad nõuded.

Infovara bilansis võib kirjeldada ka teiste õigusaktide ja andmeturbega seotud standardite järgimist. Näiteks avaliku teabe seaduse ptk-s 5^1 kirjeldatud nõudeid seonduvalt andmekogudega; andmekogudes sisalduvate andmekoosseisude töötlemiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete süsteemi, sh ISKE, mis on kehtestatud Vabariigi Valitsuse 20.12.2007 määrusega nr 252.

2.1. Infovara bilanss kui usalduse looja

Riskide vähendamine, hea maine loomine ning klientide, partnerite ja avalikkuse usalduse hoidmine muutuvad üha tähtsamaks ja mõjutavad organisatsiooni edukust kõigis sektorites. Eesmärkide täitmiseks ja konkurentsieelise saamiseks kasutavad vastutustundlikud organisatsioonid oma põhitegevust toetavaid tegevusi isegi rohkem, kui õigusaktides sisalduvad miinimumnõuded eeldavad.

Andmekaitsega seotud puudusi peetakse asjaajamise usaldusväärsuse ja kasutatavuse seisukohast probleemiks eriti just võrgukeskkonnas. Valedesse kätesse sattunud isikuandmed on oht andmesubjekti õigustele ja isikuandmete töötleja tegevusele, samal ajal loob hästikorraldatud andmekaitse klientides usalduse, mis on aluseks organisatsiooni arengule.

Infovara bilanss näitab erinevatele osapooltele, et organisatsioon täidab andmetöötlusnõudeid ja peab kinni heast andmetöötlustavast.

2.2. Infovara bilanss kui juhtkonna töövahend

Andmehalduse ühendamine juhtimisega on organisatsiooni tegevuse üks olulisemaid proovikive. Juhtkond peab kindlasti omama üldpilti organisatsiooni infokasutuse struktuuridest ja tegevuseks vajalikest andmetest ning nendevahelistest koostoimimisest.

Infovara bilanss parandab organisatsiooni juhtkonna otsuste tegemise võimekust ning aitab rahuldada klientide ja koostööpartnerite teabevajadusi. See hõlmab samuti osaliselt teabejuhtimist ning selle hulka kuuluvat riskijuhtimist ja sisekontrolli.

Andmekaitse olukorra korrapärane hindamine on üks osa organisatsiooni teabejuhtimisest. Hindamise eesmärk on tagada pakutavate teenuste toimimine ja nende kasutusmugavus, teabematerjali kvaliteet ning valitud infotehnoloogia turvalisus. Samuti aitab see tagada teenuste osutamisega seotud andmekaitse alaste juhtimis- ja haldussüsteemide tööd.

2.3. Infovara bilanss kui välis- ja sisekontrolli abivahend

Organisatsioon peab hoolitsema sisekontrolli korraldamise eest. Sisekontrolli asjakohasuse ja piisavuse eest vastutab organisatsiooni juhtkond. Organisatsiooni enda huvides on kontrollida välis- ja sisekontrolli vahenditega ka oma andmetöötlussüsteeme. Teisest küljest seonduvad sellega tugevad üldised õiguskaitsega seotud huvid. Infovara bilanss aitab täita mõlemad eesmärgid ja on abiks ka järelevalveasutuste teavitamisel.

Infovara bilanss koostatakse kontrollperioodide kaupa. See võimaldab aruandes kirjeldatud ja hinnatud asjaolusid regulaarset jälgida. Kontrollperiood võib olla kalendriaasta või mõni muu organisatsiooni vajadustele vastav ajavahemik. Infovara bilansi võib muuta sisekontrolli ja riskijuhtimise korraldamise seisukohast organisatsiooni üldise aastaaruandluse koostamise osaks.

3. Infovara bilansi koostamine

Infovara bilansi eesmärk on esitada andmetöötluse hetkeseisu kirjeldus ja hinnang andmekaitse eesmärkide täitmise kohta. Infovara bilansis selgitatakse ka andmetöötlusega seotud arenguvajadusi ja selleks vajalikke meetmeid.

Infovara bilanss võib kirjeldada näiteks:

- organisatsiooni valduses olevaid andmekogumeid;
- organisatsiooni andmetöötluse struktuuri;
- organisatsiooni valduses olevate andmete kvaliteeti ja käideldavust;
- andmete töötlemisel rakendatavaid toiminguid ja põhimõtteid;
- kuidas andmeid kaitstakse;
- kuidas kontrollitakse andmete kasutamist;
- kuidas on tagatud andmesubjektide õigused.

Infovara bilanss sisaldab ka hinnangut arendamist vajavate valdkondade ja meetmete kohta.

Infovara bilansi koostamisel võiksid organisatsioonis osaleda vähemalt infotehnoloogia, isikuandmete kaitse, infoturbe ning tegeliku andmetöötluse ja teenuste eest vastutajad.

3.1. Infovara bilansi andmed

Infovara bilansis sisalduvad andmed võivad organisatsiooni tegevusalast ja tegevuse iseloomust sõltuvalt olla erinevad. Järgnevalt toome näiteid teemadest, mida võiks infovara bilansis käsitleda.

3.2. Organisatsiooni valduses olevad andmekogumid

Organisatsioonides kogutakse ja töödeldakse andmeid paljudes infosüsteemides ja rakendustes. Juhtkonnal ei ole alati ülevaadet, millised andmed organisatsiooni valduses on. Andmete töötlemine üksteisest eraldatud infosüsteemides nõuab rohkesti ressursse ja ohustab andmekaitse eesmärkide täitmist.

Isikuandmete töötlemise seisukohast on tähtis hinnata eri otstarbel kogutud isikuandmeid ja nende andmete koosseisu. Hea andmetöötlustava vaatenurgast peaks organisatsioonil olema oma infosüsteemidest selge ülevaade, samuti tuleks hoolitseda andmete kvaliteedi ja kättesaadavuse eest.

Andmetöötluse analüüsi käigus on otstarbekas hinnata andmeturbe taset, konfidentsiaalsust ja andmete tundlikkust. Oluline on analüüsida ka andmebaaside vahelisi andmevooge, sest üha suuremate andmevoogude juhtimine tõstatab küsimuse näiteks andmete omaniku kohta. Andmebaaside ja andmevoogude kirjelduse võib koostada infovara bilansi jaoks, samal ajal võivad need olla organisatsioonis olemas ka eraldi hallatavate struktuurikirjelduste või muude vastavate kirjeldustena.

Infovara bilanss võib sisaldada organisatsiooni põhiliste andmebaaside ja andmevoogude kirjeldust ning hinnangut andmete kvaliteedile. Andmete kasutamise seisukohast võidakse seal kirjeldada ka nende põhinäitajaid, näiteks saadud ja edastatud andmeid ning andmete edastuskordade hulka. Andmete kvaliteedi hindamine seondub tihedalt hinnangu andmisega nende väärtusele ja kasutatavusele.

Andmete kvaliteeti võib infovara bilansis hinnata erinevatel alustel, näiteks:

- kvaliteedi hindamisega seonduvad toimingud ja kriteeriumid;
- kvaliteedi hindamisel saadud tulemused, näiteks andmete:
    - õigsus
    - vajalikkus
    - täielikkus
    - asjakohasus

3.3. Andmetöötlusele kohalduvad põhimõtted ja kord

Organisatsioon peaks andmete töötlemisel järgima:

- andmete töötlemist mõjutavaid põhilisi õigusakte;
- tegevuspõhimõtteid ja eeskirju;
- andmeturbe ja järjepidevuse kavasid;
- muid andmetöötlust puudutavaid norme;
- andmetöötlust puudutavate sisseostetud teenustega seotud toiminguid ja lepinguid;
- infosüsteemide haldamise ja hankimisega seotud tegevusi ja lepinguid.

Andmetöötluse tegevuspõhimõtete puhul võib hinnata näiteks:

- andmete saamise ja edastamisega seotud toiminguid;
- kasutusõiguste haldamist;
- eelkõige elektroonilise andmeedastusega seotud andmeturbenõudeid.

Infovara bilansis hinnatakse, kas organisatsiooni personal valdab vajalikku teavet kasutatavate andmete avalikkuse, konfidentsiaalsuse ja isikuandmete kaitsmisel järgitavate tegevuste ning andmeturbe korralduse ja ülesannete jagunemise kohta. Samuti kirjeldatakse, kuidas on korraldatud töötajate andmete kasutamise alane juhendamine ja koolitamine ning kuidas nende teadmisi värskendatakse.

3.4. Infoturve

Infovara bilansis võib kirjeldada, kuidas vastutav töötleja rakendab isikuandmete kaitseks vajalikke tehnilisi ja organisatoorseid meetmeid, et takistada andmetele kõrvaliste isikute juurdepääsu ning hoida ära nende tahtmatu või ebaseaduslik hävitamine, muutmine, edastamine, ülekandmine ja muu ebaseaduslik kasutamine.

Infovara bilansis võib hinnata:

- isikuandmete kaitse põhimõtteid ja tegevusi;
- infoturbe põhilisi eesmärke ja vahendeid;
- infoturbe standardeid;
- sise- ja välishindamisi;
- riskijuhtimist;
- infoturbe korraldust;
- vastutust ja arendusprotsessi.

3.5. Andmetöötluse kontroll ja järelevalve

Organisatsioon peab tagama, et hea andmetöötlustava rakendamise eeskirju ja juhiseid järgitakse ning seda kontrollitakse. Selleks vajalikke meetmeid rakendatakse viisil, mis kindlustab eri poolte õiguskaitse.

Andmetöötluse järelevalve võib olla üks osa organisatsiooni sisekontrollist ja riskijuhtimisest. Ka järelevalve tulemusi ja nende põhjal kavandatud meetmeid on põhjust hinnata.

Infovara bilansis võib kirjeldada muu hulgas:

- andmetöötlusega seotud riskide hindamist ja haldamist;
- andmebaaside ja andmevoogude kvaliteedi kontrollimiseks rakendatavaid meetmeid;
- andmete kasutamise protsesside järelevalveks rakendatavaid meetmeid;
- organisatsiooni töötajate ja koostööpartnerite andmetöötluse kontrollimiseks rakendatavaid meetmeid;
- järelevalve ja kontrolli alusel rakendatud meetmeid ja arendustegevust.

Sisekontrolli kõrval võib bilansis välja tuua ka väliste järelevalveasutuste ja kohtute asjakohased otsused, mis kontrollperioodil organisatsiooni kohta on tehtud, ning kirjeldada nende mõju organisatsiooni tegevusele. Lisaks võib infovara bilansis hinnata andmetöötluse järelevalve ja kontrolli põhjalikkust ning arendusvajadust.

3.6. Andmesubjekti õiguste tagamine

Andmesubjekti õiguste tagamist saab hinnata isikuandmete kaitse seaduses sätestatud nõuete põhjal. Näiteks võib hinnata andmesubjekti taotluste arvu seoses õigusega saada teavet ja enda kohta käivaid isikuandmeid (IKS § 19) ning õigusega nõuda andmete töötlemise lõpetamist, samuti nende parandamist, sulgemist ja kustutamist (IKS § 21). Andmesubjekti teavitamisega seoses tuleks hinnata ka olemasolevaid isikuandmeid ja andmekaitset käsitlevate aruannete kättesaadavust.

4. Hindamine ja arendamist vajavad valdkonnad

Infovara bilansis tehakse hetkeolukorra analüüsi põhjal kindlaks arendus- ja hindamisvajadus ning nendega seonduv kontroll ja aruandlus. Arendusmeetmed võivad puudutada näiteks andmete kvaliteeti või nende kasutamise protsesse. Arendusmeetmed võivad seonduda samuti uue tehnoloogia eduka kasutuselevõtuga või valmisolekuga võtta kasutusele uusi andmetöötlusvahendeid.

Avaliku sektori asutuse puhul võib infovara bilanssi lisada ka andmeid selle kohta, kuidas on organisatsioon täitnud Vabariigi Valitsuse 20.12.2007 määruses nr 252 kehtestatud nõudeid andmekogude turvatasemete kohta.

Infovara bilansi põhjal võidakse järeldada näiteks, et:

- tegevuses ja andmete töötlemisel on järgitud head andmetöötlustava;
- andmetöötluse jälgimine ja kontroll on kehtivate õigusaktide, eeskirjade ja sisereeglite alusel õnnestunud;
- andmetöötluse järelevalve ja kontrolli käigus on leitud arendamist vajavaid valdkondi või kõrvalekaldeid, millega tegelemiseks rakendatakse eraldi loetletud meetmeid.

Infovara bilansis tehakse kindlaks näiteks järgmist:

- millistes andmetöötluse valdkondades on vajalik edasine arendus;
- määratakse kindlaks arendamist vajavad valdkonnad ja hinnatakse võimalikke lahendusi;
- hinnatakse eelmisel kontrollperioodil rakendatud arendusmeetmete õnnestumist.

Infovara bilansi võib esitada organisatsiooni juhtkonnale, töötajatele, klientidele ja teistele osapooltele või seaduse alusel järelevalvet teostavatele asutustele. Organisatsioonivälistele pooltele ei avaldata seadusest tuleneva juurdepääsupiiranguga teavet, sh ärisaladust. Samuti ei avaldata informatsiooni, mille avaldamist piirab autoriõiguse seadus. Infovara bilanss võib olla ajas muutuv, näiteks isikuandmete kaitse ja järelevalve kohta võidakse juhtkonnale esitada üksikasjalik aruanne, organisatsioonist välja suunatud aruandes võib sama teemat käsitleda seda lühidalt kokku võttes või üldisi hinnanguid andes.