Leiðbeiningar til fyrirtækja um öryggi persónuupplýsinga

Inngangur

Góð áhættugreining gerir okkur kleift að ákvarða til hvaða varúðarráðstafana þurfi að grípa til þess að tryggja öryggi gagnanna. Persónuverndarlöggjöfin tilgreinir að við vernd persónuupplýsinga þurfi að grípa til viðeigandi tæknilegra og skipulagslegra ráðstafana í samræmi við áhættu.

Slík nálgun gerir fyrirtækjum og stofnunum kleift að taka hlutlægar ákvarðanir og gera breytingar í samræmi við aðstæður. Samt sem áður er oft erfitt fyrir þann sem er óvanur slíku að gera ráðstafanir við hæfi og ganga úr skugga um að viðeigandi ráðstafanir hafi verið gerðar.

Þessar leiðbeiningar lýsa þeim lágmarksráðstöfunum sem fyrirtæki og stofnanir þurfa að gera til að uppfylla lagalegar kröfur. Athuga skal að leiðbeiningarnar eru almenns eðlis og þarf að taka mið af eðli og umfangi vinnslu persónuupplýsinga þegar öryggisráðstafanir eru ákveðnar. Þannig eru ekki gerðar sömu kröfur til fyrirtækis sem vinnur lítið magn almennra persónuupplýsinga á borð við nafn, netfang og símanúmer og t.d. heilbrigðisstofnunar sem vinnur mikið magn heilsufarsupplýsinga. Þá eru leiðbeiningarnar fyrst og fremst ætlaðar litlum og meðalstórum aðilum en þeir sem vinna með umfangsmikið magn persónuupplýsinga og/eða viðkvæmar persónuupplýsingar geta þurft að leita eftir utanaðkomandi sérfræðiaðstoð eða jafnvel afla sér vottunar. Þá taka leiðbeiningarnar ekki til sértækra öryggisráðstafana sem getur þurft að gera í ákveðnum geirum, s.s. á fjármálamarkaði eða í heilbrigðisgeiranum.

Í stuttu máli má lýsa ferlinu við að setja upp kerfi upplýsingaöryggis, á eftirfarandi hátt:

Skrásetning upplýsingaeigna

- Vélbúnaður sem notaður er við skráningu og geymslu persónugagna
- Hugbúnaður
- Tengibúnaður (Internet, ljósleiðari, innanhúsnet, þráðlaust net)
- Skjöl á pappír

Skrásetning áhrifa

- Óleyfilegur aðgangur að gögnum
- Óleyfileg breyting á gögnum
- Óvænt hindrun á aðgangi að gögnum

Skrásetning áhættu

- Aðgangur óleyfilegra innri notenda
- Aðgangur kerfisstjóra
- Aðgangur ytri árásaraðila
- Aðgangur samkeppnisaðila
- Skemmdir aðrar en af mannavöldum (eldur, vatn o.s.frv.)

Greining mögulegra áhættuþátta

- Gögn notuð á óviðeigandi hátt
- Tölvuóværu komið fyrir, vírusar, lyklaborðshlerun
- Gögnum týnt
- Gögn koma óvart fyrir augu óviðkomandi aðila
- Gögn skemmast vegna slyss eða skemmdarverks
- Gögn óaðgengileg vegna plássleysis, netstíflu

Greining úrræða

- Aðgangsstýringar
- Afritun
- Rekjanleiki aðgangs, aðgerða
- Öryggisúrræði húsnæðis
- Dulkóðun
- Upplýsingar gerðar ópersónugreinanlegar

Greining áhættustigs

- Óveruleg
- Smávægileg
- Veruleg
- Mikil

Töflu af þessu tagi má nota til að meta formlegt samband áhættuþátta:

Áhætta	Áhrif á einstaklinga	Helstu áhættuvaldar	Helsta áhætta	Núverandi eða áætluð viðbrögð	Alvarleiki	Líkur
Óæskilegur aðgangur að gögnum						
Óæskileg breyting á gögnum						
Gögn tapast						

Hér er dæmi um slíka áhættutöflu fyrir einhverja tiltekna vinnslu persónuuppýsinga. Athuga skal þó að í vissum tilvikum getur þurft að notast við aðra tíðniflokkun, t.d. ef um sérstaklega viðkvæmar persónuupplýsingar er að ræða.

Líkur/Áhrif	Lítil áhrif - 1	Miðlungs áhrif - 2	Mikil áhrif - 3	Mjög mikil áhrif - 4
Sjaldan – 1 (minna en árlega)	1	2	3	4
Nokkuð oft – 2 (<mánaðarlega)	2	4	6	8
Oft – 3 (<vikulega)	3	6	9	12
Mjög oft – 4 (<daglega)	4	8	12	16

Í þessu tilfelli eru mismunandi viðbrögð eftir margfeldi á líkum og áhættu.

Grænt (1-2) – Engra sérstakra viðbragða þörf, áhættugreining ásættanleg.

Gult (3-6) - Skoða betur, athuga hvort viðbragða sé þörf, betra öryggi, minni söfnun o.s.frv.

Rautt (7+) – Vinnsla metin of áhættusöm, þörf er á auknu öryggi eða minni vinnslu.

Uppsetning og prófun

Ef þau úrræði sem eru til staðar eða ákveðið er að setja af stað eru metin viðeigandi þarf að ganga úr skugga um að þau séu prófuð og notuð þar sem við á.

Eftirfylgni

Eftir að úrræði eru sett upp þarf að setja upp eftirlitskerfi þar sem reglum er fylgt eftir og gengið úr skugga um að úrræðum sé fylgt eftir á kerfisbundinn hátt.

Yfirlit yfir það sem þarf að gera til þess að tryggja öryggi persónuupplýsinga - öryggisráðstafanir

1. Bæta öryggisvitund notenda
2. Auðkenning notenda
3. Aðgangsstýringar
4. Atburðaskráning og atvikastjórnun
5. Öryggi vinnustöðva
6. Öryggi við fjarvinnslu
7. Verndun innra nets
8. Öryggi netþjóna
9. Öryggi vefþjóna
10. Öryggi gagna
11. Örugg langtímageymsla
12. Gagnaviðhald og gagnaeyðing
13. Eftirlit með vinnsluaðilum

14. Öryggi gagnasamskipta
15. Efnislegt öryggi
16. Eftirlit með hugbúnaðarþróun
17. Dulkóðun, rafrænar undirskriftir, heilleiki

1 – Bæta öryggisvitund notenda

Hver notandi þarf að vera meðvitaður um persónuvernd og öryggisáhættu fyrirtækis eða stofnunar

Grunnúrræði

- Aukið öryggisvitund notenda með fræðslu, áminningum, námskeiðum o.s.frv.
- Skjalið vinnsluferli og sjáið til þess að skjölun sé haldið við
- Skrifið verklagsreglur um meðhöndlun gagna og upplýsingakerfis, t.d. að
    - láta tölvudeild vita um öll brot á öryggisreglum, tilraunir til innbrota o.s.frv.
    - láta aldrei þriðja aðila fá lykilorð eða aðgangsauðkenni
    - setja ekki upp, afrita, breyta eða eyða hugbúnaði án leyfis
    - læsa vinnustöð þegar hún er ekki í notkun
    - skoða ekki, reyna að skoða eða fjarlægja gögn sem ekki tengjast verkefnum notanda
    - fylgja reglum fyrirtækis um meðferð lausra geymslumiðla og fá leyfi fyrir allri gagnaafritun
    - fylgja reglum um notkun fartækja, einkageymslusvæða, eigin tækja, Internets og síma
    - kynna sér hvernig skráningu atburða og aðgangshindrunum er háttað
    - kynna sér hvaða afleiðingar geta hlotist af brotum á reglum

Frekari úrræði

- Setjið upp gagnaflokkunarkerfi með nokkrum aðgangsstigum
- Merkið sérstaklega viðkvæm gögn
- Haldið reglulega námskeið og fundi um upplýsingaöryggi til að auka vitund
- Sjáið til þess að notendur skrifi undir trúnaðaryfirlýsingu eða að fjallað sé um trúnað í ráðningarsamningum. Ef starfsmenn falla undir lögbundna þagnarskyldu, t.d. hjá stjórnvöldum, fjármálafyrirtækjum og öðrum aðilum er rétt að taka það fram

2 – Auðkenning notenda

Til þess að notendur noti aðeins þau gögn sem þeir eiga að hafa aðgang að, þarf að auðkenna að þeir séu þeir sem þeir segjast vera áður en þeir fá aðgang að persónuupplýsingum

Auðkenni má flokka í þrennt:

- Eitthvað sem notandi veit (t.d. lykilorð)

- Eitthvað sem notandi er með (t.d. auðkenniskort eða rafræn skilríki á síma)
- Eitthvað sem notandi er eða gerir (t.d. fingrafar eða undirskrift)

Sterk auðkenning notast við eitthvað tvennt af þessu þrennu.

Grunnúrræði

- Notið auðkenni fyrir hvern notanda og bannið að fleiri notendur samnýti það. Sé slíkt óhjákvæmilegt skal fá leyfi stjórnenda og setja upp kerfi til að skrá notkun
- Fylgið reglum tölvudeildar um örugga vistun lykilorða, gildistíma og flækjustig (nota ákveðinn lágmarksfjölda stafa og tákngerða)
- Grípið til einhverra aðgerða geti notandi ekki slegið inn rétt lykilorð í ákveðnum fjölda tilrauna, t.d. að loka reikningi tímabundið eða til frambúðar eða bjóða upp á Captcha-lausn
- Látið notanda breyta lykilorði þegar hann auðkennir sig við kerfi í fyrsta sinn

Það sem þarf að forðast

- Að láta aðra hafa lykilorðið sitt eða annað auðkenni
- Að skrifa niður lykilorð í ódulkóðaða skrá, á pappír eða annars staðar þar sem aðrir geta mögulega komist í það
- Að vista lykilorð í vafra án þess að nota yfirlykilorð
- Að nota lykilorð sem vitnar í persónuupplýsingar á borð við nafn, fæðingardag o.s.frv.
- Að nota sama lykilorð á fleiri en einum stað
- Að nota sjálfgefið lykilorð áfram
- Að senda lykilorð með tölvupósti

Frekari úrræði

- Notið lykilorðageymsluforrit (e. password manager) til að halda utan um lykilorð á mismunandi stöðum og notið aðeins eitt yfirlykilorð
- Notið sterka (tvíþátta) auðkenningu þar sem því verður við komið
- Leyfið færri tilraunir til auðkenningar og lokið á notanda ef þær verða of margar
- Krefjist þess að lykilorð séu uppfærð reglulega
- Látið notendur ekki nota sjálfgefin notendanöfn eða lykilorð framleiðenda
- Vistið lykilorð dulkóðuð (öll stýrikerfi, gagnagrunnar og vafrar gera þetta)

3 – Aðgangsstýringar

Leyfið aðeins að aðgang að þeim gögnum sem notandinn raunverulega þarf aðgang að

Grunnúrræði

- Flokkið aðgang eftir þörfum og hlutverki svo að notendur hafi aðeins aðgang að þeim gögnum sem þeir þurfa, vinnu sinnar vegna
- Lokið á aðgang notenda þegar þeir hætta störfum

- Takið árlega yfirferð á aðgangi notenda til að tryggja að ekki séu til ónotaðir notendareikningar og hægt sé að skerpa á þörfum fyrir aðgang

Það sem þarf að forðast

- Að búa til eða nota sameiginlega notendareikninga
- Að gefa kerfisstjóraaðgang þeim sem ekki hafa þörf fyrir hann
- Að gefa notendum meiri aðgang en þeir hafa þörf fyrir
- Að gleyma að afturkalla auknar aðgangsheimildir sem eiga að vera tímabundnar (t.d. vegna forfalla)
- Að gleyma að ógilda aðgang notenda sem hafa hætt eða flust til í starfi

Frekari úrræði

- Setjið upp aðgangsstýringarstefnu í samræmi við vinnsluferli stofnunar eða fyrirtækis. Hún skal tilgreina:
    - Hvað skal gera þegar notendur byrja og hætta
    - Afleiðingar þess að fylgja ekki öryggisreglum
    - Hvaða leiðir eru leyfðar til að takmarka og stjórna aðgangi að persónuupplýsingum

4 – Atburðaskráning og atvikastjórnun

Til þess að hægt sé að verða var við og bregðast við ólögmætum aðgangi að persónuupplýsingum, ólögmætri notkun þeirra og rekja uppruna atvika þarf að skrá atburði í tölvukerfum og hafa formlegt ferli til að bregðast við atvikum

Grunnúrræði

- Setjið upp atburðaskrár (logga) sem skrá aðgang og auðkenningu notenda, frávik og öryggisatvik með tímasetningu
- Setjið upp ítarlegri skráningu yfir allar aðgerðir notenda þar sem um viðkvæmar upplýsingar er að ræða
- Fræðið notendur ef slík atburðaskráning er til staðar í samræmi við kröfur persónuverndarlaga
- Tryggið að aðgangi sé stýrt að skráningarvélbúnaði og hugbúnaði þannig að þeir notendur sem verið sé að skrá komist ekki í skráningarnar
- Skráið gagnavinnslu og yfirfarið slíka skráningu reglulega til að tryggja að hún sé í eðlilegu ferli
- Tryggið að þeir sem stýra skráningu láti vita af óeðlilegum atvikum og brotum
- Tilkynnið til Persónuverndar ef öryggisbrestur verður vegna aðgangs að persónuupplýsingum
- Tilkynnið til einstaklinganna sem í hlut eiga, á skýru og einföldu máli ef öryggisbrestur verður vegna ólögmæts aðgangs að persónuupplýsingum ef því fylgir mikil áhætta fyrir réttindi og frelsi þeirra

Það sem þarf að forðast

- Að nota atburðaskrár til annars en þær eru ætlaðar, t.d. er bannað að nota þær til þess að fylgjast með viðveru notenda í vinnu

5 – Öryggi vinnustöðva

Hætturnar af tölvuinnbrotum eru verulegar og vinnustöðvar eru oft aðgangspunkturinn

Grunnúrræði

- Stillið vinnustöðvar þannig að þær læsist sjálfkrafa ef þær hafa staðið ónotaðar í ákveðinn tíma
- Setjið upp eldvegg þannig að lokað sé á ónotuð port
- Uppfærið stýrikerfi, vírusvarnir og annan hugbúnað reglulega
- Stillið stýrikerfi og hugbúnað þannig að hann uppfæri sig sjálfkrafa ef unnt er
- Vistið gögn notenda á miðlægum, afrituðum disksvæðum frekar en á vinnustöðvunum sjálfum
- Takmarkið notkun lausra miðla (t.d. flakkara, minnislykla) við það allra nauðsynlegasta
- Slökkvið á sjálfvirkri keyrslu lausra miðla (e. autorun)
- Tryggið að notandi viti eða fái tilkynningu ef verið sé að eiga við vinnustöð hans utan frá

Það sem þarf að forðast

- Að nota úreltar gerðir stýrikerfa
- Að gefa notendum stjórnaðgang (e. admin rights) ef þeir kunna ekki með hann að fara

Frekari úrræði

- Forðist notkun utanaðkomandi forrita sem ekki koma frá traustum aðilum
- Forðist að nota forrit sem krefjast stjórnaðgangs
- Eyðið gögnum af vinnustöð ef hún fer til annars notanda
- Verði öryggisatvik á vinnustöð þarf að rannsaka hvernig það gerðist og hvort það hafi náð til annarra hluta tölvukerfisins
- Framkvæmið reglulegar öryggisprófanir og eftirlit
- Uppfærið hugbúnað uppgötvist öryggisgallar í honum
- Uppfærið stýrikerfi reglulega og sjálfkrafa

6 – Öryggi við fjarvinnslu

Gera þarf ráð fyrir því að fartæki geti týnst eða verið stolið og gera öryggisráðstafanir með það í huga

Grunnúrræði

- Aukið vitund notenda um hættur þess að nota fartæki (fartölvur, farsíma) og gerið ráðstafanir til að minnka þessa áhættu
- Setjið upp afritunar- eða samstillingarkerfi fyrir fartæki til þess að verjast gagnatapi
- Setjið upp dulkóðun fyrir fartæki og lausa gagnamiðla, allan diskinn ef það er hægt, annars stakar skrár eða gagnageymslur
- Krefjist þess að farsímum sé læst með auðkennisnúmeri, mynstri eða slíku
- Ef notast er við þjónustuaðila þarf hann að leggja fram fullnægjandi tryggingar fyrir því að hann geti framkvæmt öryggisráðstafanir

Það sem þarf að forðast

- Að nota umhugsunarlaust innbyggðar skýjalausnir án þess að athuga vandlega skilmála þeirra og öryggisreglur

Frekari úrræði

- Notið skjásíu á fartölvur sem eru notaðar á opinberum stöðum (svo ekki sjáist á skjá frá hlið)
- Takmarkið þau gögn sem eru geymd á fartækjum við það sem er bráðnauðsynlegt
- Gerið ráðstafanir gegn þjófnaði (öryggiskapall, sjáanlegar merkingar) og til þess að lágmarka áhrif hans (sjálfvirk læsing, dulkóðun)
- Dulkóðið tengingu og gögn og læsið tækinu eftir notkun þegar fartæki eru notuð til að safna gögnum á ferðalagi (gegnum vafra, tölvupóst)

7 – Verndun innra nets

Leyfið aðeins þær nettengingar sem þörf er á

Grunnúrræði

- Takmarkið Internetaðgang með því að loka fyrir ónauðsynlegar þjónustur
- Dulkóðið öll þráðlaus net og setjið á þau flókin lykilorð. Net sem eru opin gestum skulu vera aðskilin frá innri netum
- Krefjist þess að VPN sé notað fyrir fjartengingar inn á innra net, helst með sterkri (tvíþátta) auðkenningu
- Tryggið að stjórnborð hugbúnaðar eða þjónusta séu ekki aðgengileg beint frá Internetinu

Það sem þarf að forðast

- Að nota ódulkóðaðar tengingar á borð við *telnet* til þess að tengjast netbúnaði. Notið öruggar tengingar eins og *ssh* (e. Secure Socket Shell) eða beinan aðgang með snúru
- Að setja upp þráðlaust net með WEP dulkóðun. Notið ávallt WPA2 eða nýrri dulkóðun

Frekari úrræði

- Ýmsar evrópskar stofnanir á sviði persónuverndar og upplýsingaöryggis (ICO, ENISA, ANSSI) hafa gefið út leiðbeiningar (á ensku) um öryggi vefsvæða, samskiptastaðalsins TLS (e. Transport Layer Security) og þráðlausra neta, sem hægt er að kynna sér
- Mögulegt er að bera rafræn kennsl á tæki og hindra óþekkt tæki frá því að tengjast netinu
- Árásargreining (e. Intrusion Detection System) getur greint netumferð og stöðvað hugsanlegar árásir á búnað. Það þarf að upplýsa notendur um það ef umferð þeirra er greind skv. persónuverndarlöggjöfinni
- Niðurskipt netkerfi getur dregið úr áhrifum þess að einstakir hlutar þess verði fyrir inngripi. Aðskilja skal ytra net (DMZ, De-Militarized Zone) þar sem vefþjónar, póstþjónar o.þ.h. eru hýstir, frá innra neti

8 – Öryggi netþjóna

Að tryggja öryggi netþjóna er fyrir öllu þar sem þeir hýsa mikið af gögnum

Grunnúrræði

- Gefið aðeins hæfu fólki stjórnaðgang og aðgang að stjórnborðum og stjórntækjum
- Notið notanda með minni aðgang fyrir önnur störf
- Hafið lykilorðareglur fyrir stjórnnotendur og skiptið um lykilorð þegar einhver þeirra hættir
- Setjið inn öryggisuppfærslur án tafar þegar þær berast
- Notið sérgagnagrunnsnotanda fyrir hvert forrit
- Takið regluleg afrit og prófið þau reglulega
- Setjið upp TLS dulkóðun og auðkenningu fyrir allar vefþjónustur

Það sem þarf að forðast

- Að nota ótryggar þjónustur (ódulkóðuð auðkenning, ódulkóðaður gagnastraumur)
- Að setja gagnagrunna á vélar sem einnig hýsa aðrar þjónustur (vefi, póst, spjall)
- Að láta gagnagrunna vera aðgengilega beint frá netinu
- Að fjölnota aðgang (notendur sem eru notaðir af fleiri en einni manneskju eða þjónustu)

Frekari úrræði

- Aðskiljið kerfi sem vinna viðkvæmar upplýsingar frá öðrum kerfum
- Í stærri netkerfum ætti kerfisstjórn að fara fram frá aðskildu stjórnneti sem er tryggt með sterkri auðkenningu og atburðaskráningu
- Greinið og skoðið viðkvæm kerfi með netgreiningartólum eins og nmap (e. Network Mapper) til að uppgötva mögulegar öryggisholur. Setjið upp kerfi til að takmarka auðkenningartilraunir
- Takmarkið aðgang að stjórnportum og stjórnborðum hugbúnaðar og vélbúnaðar

9 – Öryggi vefþjóna

Öll vefsvæði þurfa að auðkenna sig og réttmæti þeirra gagna sem þau miðla eða safna

Grunnúrræði

- Setjið upp TLS dulkóðun
- Skyldið TLS á öllum síðum sem safna eða sýna gögn sem ekki eiga að vera opin almenningi
- Lokið fyrir umferð á öllum portum sem ekki er þörf á
- Gefið aðeins hæfu fólki stjórnaðgang og takmarkið notkun stjórnnotenda við slíkt
- Fáið samþykki notanda ef þið eruð að safna vefkökum sem eru ekki bráðnauðsynlegar fyrir virkni vefsins
- Gerið vefkerfi ekki flóknara en það þarf að vera, fjarlægið ónotuð undirkerfi og uppfærið þá hluta sem eru notaðir

Það sem þarf að forðast

- Að setja persónuupplýsingar á borð við notendanöfn eða lykilorð í slóðir (URL)
- Að nota ódulkóðaðar þjónustur og auðkenningu
- Að nota netþjóna sem vinnustöðvar, sérstaklega ekki nota þá til að vafra, sækja póst eða spjall
- Að setja gagnagrunna á þjóna sem eru beint aðgengilegir frá Internetinu
- Að láta marga samnýta sama notandann (t.d. administrator, root)

Frekari úrræði

- Kynnið ykkur löglega og rétta notkun vefkaka og aðra slíka rakningu notkunar
- Skannið netþjóna reglulega með tilliti til öryggis og þjónusta
- Kynnið ykkur reglur ICO, ENISA, ANSSI um uppsetningu TLS dulkóðunar á vefþjónum

10 – Öryggi gagna

Afrita þarf gögn og prófa afritin reglulega. Gera þarf aðgerðaráætlun til að tryggja samfelldan rekstur ef til gagnataps eða vélbúnaðarbilunar kemur

Grunnúrræði

- Setjið upp reglulega afritun. Helst daglega síhlutaafritun (e. progressive incremental backup) og fulla afritun öðru hverju, t.d. á þriggja mánaða fresti
- Geymið afritin utan fyrirtækis eða stofnunar, helst í eld- og vatnsvörðu rými
- Verjið afritin jafn vel og netþjónana sjálfa, með dulkóðun og aðgangsstýringum
- Dulkóðið afritunarstrauminn ef hann fer yfir netið
- Gerið aðgerðaráætlun um hvernig skal bregðast við gagnatapi eða öðrum áföllum
- Tryggið að notendur, hýsingaraðilar og undirverktakar viti hvern eigi að hafa samband við þegar óhöpp verða
- Prófið afrit og endurheimt þeirra reglulega til að tryggja að þau séu í lagi og rétt
- Notið rafgeymi (UPS) til að verja tækjabúnað fyrir rafmagnsleysi
- Tryggið að gögn séu geymd á margföldum diskum (RAID) til öryggis

Það sem þarf að forðast

- Ekki geyma afrit á sama stað og vélarnar sem hýsa frumgögnin. Elds- eða vatnstjón gæti t.d. orsakað að hvoru tveggja tapaðist í einu

Frekari úrræði

- Hugleiðið að gera aðgerðaráætlun um viðbrögð við helstu mögulegu áföllum. Leiðbeiningar um slíkt má finna víða á netinu
- Ef gögnin eru mjög mikilvæg má hugleiða að koma upp tvöföldu netþjónakerfi á sitt hvorum staðnum

11 – Örugg langtímageymsla

Gögn sem ekki eru lengur notuð reglulega en sem gætu verið nauðsynleg í framtíðinni, t.d. af lagalegum ástæðum, þarf stundum að vista í langtímaskjalasafni

Grunnúrræði

- Skilgreinið þarfir skjalasafnsins, hvað skal geyma? Hvar? Hversu lengi?
- Skilgreinið aðgangsþarfir skjalasafnsins
- Þegar að því kemur að eyða gögnum endanlega, gangið úr skugga um að þeim hafi raunverulega verið eytt að fullu

Það sem þarf að forðast

- Að nota geymslugögn með ónógan líftíma, t.d. er ekki hægt að treysta því að gögn séu aðgengileg á skrifanlegum CD og DVD diskum lengur en 4-5 ár
- Að geyma eldri gögn í gagnagrunni sem er í fullri notkun
- Að geyma pappírsgögn í plastmöppum eða með bréfaklemmum/heftum

Frekari úrræði

- Í lögum um opinber skjalasöfn eru afhendingarskyldir aðilar til Þjóðskjalasafns/héraðsskjalasafna skilgreindir, t.d. ráðuneyti, dómstólar, stofnanir og sveitarfélög o.fl. Heimildir þessara aðila til að eyða upplýsingum eru mjög takmarkaðar. Þeim ber jafnframt að haga skjalavörslu sinni í samræmi við reglur Þjóðskjalasafns (https://skjalasafn.is/reglur_og_leidbeiningar)
    - Meðal annars þarf að ganga úr skugga um að möppur séu sýrufríar og að gögn séu ekki geymd í plastmöppum eða innihaldi bréfaklemmur, þar sem slíkt getur eyðilegt gögn sem skulu fara í langtímavarðveislu

12 – Gagnaviðhald og gagnaeyðing

Gagnageymslur þarf að skipuleggja til að hafa stjórn á aðgangi að þeim. Gögnum þarf að eyða áður en vélbúnaði er eytt eða hann seldur

Grunnúrræði

- Haldið miðlægt utan um það hvernig gagnamiðlar eru afritaðir, fluttir til eða þeim eytt
- Setjið klausu um upplýsingaöryggi í viðhaldssamninga hýsingaraðila og verktaka
- Látið hæft starfsfólk fylgjast með verkum þriðju aðila
- Hafið skýrar verklagsreglur um gagnaeyðingu og farið eftir þeim
- Eyðið gögnum á öruggan hátt af vélbúnaði áður en honum er hent, hann seldur, sendur til viðgerðar eða í lok leigutímabils

Það sem þarf að forðast

- Að setja upp hugbúnað fyrir fjarvinnslu sem er óöruggur, t.d. notast við ódulkóðaðar gagnatengingar
- Að endurnýta, selja eða henda gagnamiðlum án þess að eyða gögnum af þeim á öruggan hátt

Frekari úrræði

- Nota skal vottaðan gagnaeyðingarhugbúnað

13 – Eftirlit með vinnsluaðilum

Tryggja þarf örugga meðferð persónugagna sem eru unnin af undirverktökum eða þjónustuaðilum

Grunnúrræði

- Notið aðeins vinnsluaðila sem geta tryggt nægilega hæfni, þekkingu og bolmagn
- Látið vinnsluaðila skrifa undir trúnaðaryfirlýsingu
- Kannið og skjalið hvernig vinnsluaðilinn hyggst tryggja öryggi gagna, m.a. dulkóðun gagna og gagnastrauma, aðgangsstýringu, auðkenningu og atburðaskráningu
- Gerið skriflegan samning við vinnsluaðilann sem útlistar viðfangsefni, umfang, tímabil og tilgang vinnslunnar auk skyldna hvers aðila. Persónuvernd hefur útbúið fyrirmynd að vinnslusamningi sem hægt er að nota. Mikilvægt er að tryggja auðkenningu, rétta meðferð upplýsinga (eyðingu eða skil) að vinnslu lokinni og tilkynningaskyldu ef frávik verða

Það sem þarf að forðast

- Að láta vinnsluaðila hefja vinnslu persónuupplýsinga án þess að hafa gildan, skriflegan samning þar að lútandi
- Að nota skýjaþjónustu án þess að hafa upplýsingar um staðsetningu gagnageymslna eða án þess að tryggja lögmæta gagnaflutninga utan EES-svæðisins

Frekari úrræði

- Sjá 28. gr. pvrg.
- Fyrirmynd að vinnslusamningi
- Fá staðfestingu um fullnægjandi tryggingar

14 – Öryggi gagnasamskipta

Tryggið öryggi við allan flutning persónuupplýsinga og munið að tölvupóstkerfi og rafræn samskiptakerfi eru ekki öruggir farvegir fyrir samskipti án frekari ráðstafana og að allir sem hafa aðgang að viðkomandi netþjónum gætu haft aðgang að gögnunum

Grunnúrræði

- Dulkóðið gögn sem á að senda á geymslumiðli (USB, DVD, flakkara) til þriðja aðila
- Dulkóðið gögn sem á að senda yfir netið með því að nota HTTPS, SFTP
- Sendið ekki lykilorð dulkóðaðra skráa með sjálfum skránum
- Ef nota þarf fax, sendið aðeins á fax sem hefur tryggt aðgengi

Það sem þarf að forðast

- Að senda ódulkóðuð gögn með almennum tölvupósti

Frekari úrræði

- Ef kostur er, setjið upp lyklaða dulkóðun og rafræna undirritun með opinberum og einkalyklum

15 – Efnislegt öryggi

Tryggið öryggi húsnæðis þar sem gagnaþjónar og netbúnaður eru hýst. Koma þarf í veg fyrir óleyfilegan aðgang eða hamla honum eins og kostur er

Grunnúrræði

- Setjið upp þjófavarnarkerfi og tryggið að fylgst sé með því
- Setjið upp reykskynjara og eldvarnarbúnað og yfirfarið árlega
- Aðskiljið svæði eftir viðkvæmni, t.d. með því að takmarka aðgang að tölvurými
- Haldið lista yfir þá sem hafa aðgang að hverju svæði og haldið listunum við
- Setjið aðgangsreglur, t.d. með því að láta starfsmann alltaf fylgja utanaðkomandi aðilum
- Verndið tölvubúnað með sértækum búnaði, t.d. eldvarnarbúnaði, upphækkuðum hillum til að forða vatnsskemmdum, tvöföldu rafkerfi og loftræstingu

Það sem þarf að forðast

- Að vanáætla stærð eða viðhaldsþörf tölvurýma. Ef kerfi á borð við rafkerfi, rafhlöður eða loftræstingu bregst, getur tölvubúnaður hætt að virka, gögn geta glatast eða aðgangur að þeim opnast

Frekari úrræði

- Skrá aðgang að rýmum þar sem persónuupplýsingar eru geymdar. Minnið starfsfólk á að slík skráning sé í gangi
- Sjáið til þess að aðeins réttmætu starfsfólki sé hleypt inn á viðkvæm svæði og að það þurfi að bera á sér sjáanlegt auðkenni (aðgangskort með mynd)

- Gestir, t.d. tæknimenn, hafi takmarkaðan aðgang og að koma og brottför þeirra séu skráð
- Farið reglulega yfir aðgangsheimildir viðkvæmra svæða og breytið þeim þegar þörf krefur

16 – Eftirlit með hugbúnaðarþróun

Öryggi og persónuvernd þurfa að vera innbyggð í alla hugbúnaðarþróun frá upphafi. Nauðsynlegt er að hugbúnaður veiti notendum stjórn yfir upplýsingum sínum og að hann sé verndaður fyrir villum, gagnatapi, óleyfilegum breytingum eða misnotkun

Grunnúrræði

- Byggið persónuvernd og öryggi inn í hönnun hugbúnaðar frá upphafi. Þetta getur haft áhrif á það hvaða leiðir og lausnir séu valdar
- Tryggið alltaf að mesta öryggi sé sjálfgefin stilling í hugbúnaði sem ætlaður er almenningi
- Forðist innsláttarsvið með frjálsum texta eða athugasemdum ef hægt er
- Setjið upp aðskilið þróunarumhverfi fyrir þróun og forritun og notið skálduð eða ópersónugreinanleg gögn

Það sem þarf að forðast

- Að nota raunveruleg gögn við þróun eða prófun. Nota skal skálduð gögn alls staðar þar sem því verður komið við
- Að þróa hugbúnað án þess að taka tillit til öryggis og persónuverndar

Frekari úrræði

- Aðeins skal safna þeim lágmarksgögnum sem nauðsynleg eru, t.d. ef aðeins er þörf fyrir fæðingarár skal ekki láta forritið sækja mánuð og dag líka
- Velja skal geymsluform eftir þeim geymslutíma sem áætlaður er, t.d. ef ætlunin er að geyma gögnin í 20 ár er heppilegra að velja opið gagnaform sem líklegra er til að vera stutt til lengri tíma
- Aðgangsstýring skal innbyggð í hugbúnaðarþróun frá upphafi
- Í mörgum tilfellum er heppilegt að tryggja kóða með rafrænni undirskrift til að tryggja að ekki hafi verið átt við hann

17 – Dulkóðun, rafrænar undirskriftir, heilleiki

Mikilvægt er að varðveita heilindi, leynd og heilleika gagna. Hakkaföll má nota til að tryggja heilindi gagna, uppruna má tryggja með rafrænni undirskrift og leynd með dulkóðun

Grunnúrræði

- Notið þekkt og viðurkennd reiknirit (algóritma) og uppfærið eftir þörfum (geta breyst og munu breytast)
    - SHA-256, SHA-512 eða SHA-3 sem hakkaföll
    - HMAC/SHA-256, bcrypt, scrypt eða PBKDF2 til að geyma lykilorð
    - AES eða AES-CBC fyrir samhverfa dulkóðun
    - RSA-OAEP fyrir ósamhverfa dulkóðun
    - RSA-SSA-PSS fyrir rafrænar undirskriftir

Það sem þarf að forðast

- Að nota úrelt reiknirit eins og DES og 3DES fyrir dulkóðun eða MD5 eða SHA1 sem hakkaföll
- Að rugla saman hakkafalli og dulkóðun eða að telja að hakkafallið eitt nægi til að tryggja gagnaleynd. Þó að hakkaföll séu “einstefnu”, þ.e. erfitt að snúa til baka, er stundum mögulegt að endurgera gögn úr hakkinu. Hakkaföll eru hönnuð til að vera hraðvirk og því er stundum mögulegt að hakka öll möguleg inngögn (t.d. lykilorð) og ná þannig gögnunum

Frekari úrræði

- Skoðið rafræn skilríki og staðfestið að notkun þeirra sé í samræmi við það sem ætlað er, að þau séu í gildi og að þau hafi gilda staðfestingarkeðju
- Notið staðfesta hugbúnaðar- og dulkóðunarpakka
- Notið samþykktar og staðfestar aðferðir til dulkóðunar, t.d.
    - GNU Privacy Guard (GPG)
    - Lausnir staðfestar af ENISA
    - VeraCrypt hugbúnað

ÖRYGGISMAT FYRIR FYRIRTÆKI EÐA STOFNUN

Það sem þarf að gera		Grunnúrræði	✓
1	**Bæta öryggisvitund notenda**	Aukið öryggisvitund með fræðslu, áminningum og námskeiðum	
		Skjalið vinnsluferli og sjá til þess að skjölun sé haldið við	
2	**Auðkenning notenda**	Notið sértækt auðkenni fyrir hvern notanda og ekki samnýta það	
		Fylgið reglum um örugga vistun, aldur og flækjustig lykilorða	
		Bregðist við ef notandi getur ekki slegið inn rétt lykilorð	
		Krefjist þess að notandi breyti lykilorði í fyrsta sinn	
3	**Aðgangsstýringar**	Flokkið aðgang eftir þörfum og hlutverki notenda	
		Lokið á aðgang þeirra sem hætta störfum	
		Takið reglulega yfirferð yfir notendareikninga	
4	**Atburðaskráning og atvikastjórnun**	Setjið upp atburðaskrár yfir aðgang, frávik og atvik	
		Athugið hvort ítarlegri atburðaskráningar sé þörf	
		Látið notendur vita af atburðaskráningu	
		Tryggið aðgengi að atburðaskrám	
		Skráið gagnavinnslu og óeðlileg atvik	
		Tilkynnið Persónuvernd og/eða öðrum stjórnvöldum (t.d. lögreglu, FME, CERT-IS) öryggisbrest	
5	**Öryggi vinnustöðva**	Stillið vinnustöðvar þannig að þær læsist sjálfkrafa	
		Uppfærið stýrikerfi, vírusvarnir og annan hugbúnað reglulega	
		Setjið upp sjálfvirkar uppfærslur á stýrikerfi og hugbúnaði	
		Vistið notendagögn miðlægt	
		Takmarkið notkun lausra geymslumiðla	
		Slökkvið á sjálfvirkri keyrslu lausra geymslumiðla	
		Tryggið að notandi viti af því ef átt er við vinnustöð utan frá	
6	**Öryggi við fjarvinnslu**	Aukið vitund notenda um hættur þess að nota fartæki	
		Setjið upp afritun fyrir fartæki	
		Setjið upp dulkóðun fyrir fartæki	
		Krefjist þess að fartækjum sé læst með auðkenningu	
7	**Verndun innra nets**	Takmarkið netumferð við það nauðsynlegasta	
		Setjið upp dulkóðun fyrir þráðlaus net	
		Krefjist þess að VPN sé notað fyrir allar fjartengingar	
8	**Öryggi netþjóna**	Gefið aðeins hæfu fólki kerfisstjóraaðgang	
		Setjið upp öryggisuppfærslur án tafar	
		Takið regluleg afrit og prófið þau	
9	**Öryggi vefþjóna**	Setjið upp TLS dulkóðun	
		Tryggið að lykilorð og notendanöfn séu ekki í vefslóðum	
		Tryggið að notendagögn séu ekki tekin inn án skoðunar	
10	**Öryggi gagna**	Setjið upp öruggt afritunarkerfi	
		Geymið afritin á öruggum stað	
		Tryggið öruggan flutning afrita	
		Gerið reglulegar prófanir á afritum	
11	**Örugg langtímageymsla**	Setjið upp aðgangskerfi fyrir langtímaafrit	
		Eyðið langtímaafritum á öruggan hátt þegar þar að kemur	
12	**Gagnaviðhald og gagnaeyðing**	Setjið upp skráningarkerfi fyrir gagnaviðhald og eyðingu	
		Látið hæft starfsfólk fylgjast með vinnu þriðja aðila	
		Eyðið öllum gögnum af vélbúnaði sem er eytt eða seldur	
13	**Eftirlit með vinnsluaðilum**	Gerið sértækan samning við alla vinnsluaðila	
		Gerið samning um eyðingu eða skil gagna eftir vinnslu	
		Eyðið gögnum af vélbúnaði sem er skilað, eytt eða seldur	
14	**Öryggi gagnasamskipta**	Dulkóðið gögn sem á að senda yfir netið	
		Tryggið ávallt réttan viðtakanda	
		Sendið lykilorð og slíkt ekki með sjálfum gögnunum	
15	**Efnislegt öryggi**	Læsið ávallt dyrum að kerfisrýmí og takmarkið aðgang	
		Setjið upp þjófavarnarkerfi og prófið það reglulega	
16	**Eftirlit með hugbúnaðarþróun**	Byggið upplýsingaöryggi inn í hugbúnað frá upphafi	
		Forðist innsláttarsvið með frjálsum texta	
		Prófið hugbúnað með skálduðum gögnum	
17	**Dulkóðun, rafrænar undirskriftir, heilleiki**	Notið þekktar og viðurkenndar dulkóðanir	
		Geymið auðkenni og dulkóðunarlykla á öruggan hátt	