Persónuvernd

LEIÐBEININGAR UM TILKYNNINGAR UM ÖRYGGISBROT

Almennt

Ein af þeim nýjungum, sem kynntar eru til sögunnar með persónuverndarreglugerð ESB 2016/679 (pvrg.), felur í sér að tilkynna þarf um öryggisbrot til Persónuverndar. Í vissum tilvikum þarf einnig að upplýsa þá einstaklinga, sem upplýsingarnar varða, um að öryggisbrot hafi orðið hvað varðar persónuupplýsingar þeirra. Leiðbeiningar þessar byggja á leiðbeiningum sk. 29. gr. vinnuhóps ESB, sem skipaður er öllum forstjórum persónuverndarstofnana ESB, og hefur Persónuvernd á Íslandi þar áheyrnaraðild.

Í ákvæðum 33. gr. og 34. gr. persónuverndarreglugerðarinnar er fjallað um öryggisbrot.

Efnisyfirlit

1. Hvað er öryggisbrot? 2
2. Hvenær á að tilkynna Persónuvernd um öryggisbrot? 2
3. Hvenær telst ábyrgðaraðili hafa orðið var við öryggisbrot? 3
4. Hverjar eru skyldur vinnsluaðila? 5
5. Hvaða upplýsingar er skylt að veita Persónuvernd? 5
6. Þarf tilkynning til Persónuverndar að innihalda allar upplýsingar um öryggisbrot? 6
7. Í hvaða tilvikum þarf ekki að senda Persónuvernd tilkynningu um öryggisbrot? 6
8. Hvenær þarf að upplýsa einstaklinga? 7
9. Hvaða upplýsingar er skylt að veita einstaklingum? 7
10. Hvernig skal hafa samband við einstaklinga? 8
11. Hvenær þarf ekki að upplýsa einstaklinga? 8
12. Hvaða atriði þarf að hafa í huga við mat á áhættu? 9
13. Skrá yfir öryggisbrot 10

1. útgáfa, febrúar 2018

1. Hvað er öryggisbrot?

A. Skilgreining á öryggisbroti samkvæmt persónuverndarreglugerðinni:

Öryggisbrot er brot á öryggi sem leiðir til óviljandi eða ólögmætrar eyðingar persónuupplýsinga, sem eru sendar, varðveittar eða unnar á annan hátt, **eða** að þær glatist, breytist, verði birtar eða aðgangur veittur að þeim í leyfisleysi.

B. Tegundir öryggisbrota:

1. **Öryggisbrot sem felur í sér brot á trúnaði (e. Confidentiality breach)** – óheimil miðlun eða miðlun fyrir mistök á persónuupplýsingum eða óheimill aðgangur að þeim.
2. **Öryggisbrot sem leiðir til þess að upplýsingar verða óaðgengilegar (e. Availability breach)** – tap á aðgengi að persónuupplýsingum eða eyðilegging þeirra fyrir mistök eða án heimildar.
3. **Öryggisbrot sem felur í sér breytingu á persónuupplýsingum (e. Integrity breach)** – breyting á persónuupplýsingum fyrir mistök eða án heimildar.

Hér þarf að hafa í huga að öryggisbrot getur falið í sér alla framangreinda flokka.

Þótt persónuupplýsingar séu eingöngu óaðgengilegar um tíma felur það engu að síður í sér öryggisbrot, sem þarf að skrá sem slíkt. Þá er einnig mikilvægt að ábyrgðaraðili meti allar hugsanlegar afleiðingar öryggisbrots. Þó fer eftir aðstæðum hvort nauðsynlegt sé að tilkynna um það til Persónuverndar og upplýsa hina skráðu.

Dæmi
Þegar gögnum hefur verið eytt, annaðhvort óvart eða af einstaklingi án heimildar, eða þegar dulkóðunarlykill, sem tengir saman auðkenni einstaklinga og dulkóðaðar upplýsingar, tapast.

Dæmi
Þegar um er að ræða verulegt rof á reglubundinni þjónustu fyrirtækis, til dæmis þegar tölvuárás leiðir til rafmagnsleysis eða að persónuupplýsingar verða óaðgengilegar, annaðhvort varanlega eða tímabundið.

Dæmi
Sú staðreynd að heilsufarsupplýsingar á spítala eru óaðgengilegar um tíma getur leitt til áhættu fyrir réttindi og frelsi einstaklings, til dæmis ef skurðaðgerð frestast vegna þessa.

Dæmi
Tölvukerfi fjölmiðlafyrirtækis er óaðgengilegt í nokkra klukkutíma vegna rafmagnsleysis sem leiðir til þess að ekki er hægt að senda tímarit til áskrifenda. Þessi aðstaða felur tæpast í sér áhættu fyrir réttindi og frelsi einstaklinga.

Dæmi
Tölvukerfi ábyrgðaraðila er sýkt af tölvuvírus, sem felur í sér að öll gögn eru dulkóðuð, þar til lausnargjald hefur verið greitt. Þetta getur leitt til þess að gögnin eru tímabundið óaðgengileg. Innrás átti sér engu að síður stað og tilkynningar gæti verið krafist ef atvikið flokkast sem trúnaðarbrot, þ.e. persónuupplýsingar verða aðgengilegar óviðkomandi, sem felur í sér áhættu fyrrir réttindi og frelsi einstaklinga.

Þá er einnig mikilvægt að ábyrgðaraðili meti allar hugsanlegar afleiðingar öryggisbrots. Þó fer eftir aðstæðum hvort nauðsynlegt sé að tilkynna um það til Persónuverndar og upplýsa hina skráðu.

C. Mögulegar afleiðingar öryggisbrots

Tilkynni ábyrgðaraðili ekki um brot, annaðhvort til Persónuverndar eða hinna skráðu, þrátt fyrir að skilyrði 33. og/eða 34. gr. séu uppfyllt, þarf Persónuvernd að taka ákvörðun um beitingu þeirra valdheimilda sem henni eru veittar í persónuverndarreglugerðinni, svo sem álagningu stjórnvaldssektar eða að gera ráðstafanir til úrbóta.

Ástæður þess að ekki er tilkynnt um öryggisbrot geta verið að:

a) viðeigandi öryggisráðstafanir eru ekki til staðar, eða

b) eftirfylgni við þær er ábótavant.

Vegna þess að um er að ræða tvö aðskilin brot getur Persónuvernd ákveðið að nýta valheimildir sínar, annars vegar vegna þess að ábyrgðaraðila hafi láðst að tilkynna um brot (33. og 34. gr.) og hins vegar vegna skorts á viðeigandi öryggisráðstöfunum (32. gr.).

2. Hvenær á að tilkynna Persónuvernd um öryggisbrot?

Ef um er að ræða öryggisbrot við meðferð persónuupplýsinga skal ábyrgðaraðili, án ótilhlýðilegrar tafar, og, ef mögulegt er, eigi síðar en 72 klst. eftir að hann verður brotsins var, tilkynna til Persónuverndar um brotið, nema ólíklegt þyki að það leiði til áhættu fyrir réttindi og frelsi einstaklinga.

Sé Persónuvernd ekki tilkynnt um brotið innan 72 klst. skulu ástæður fyrir töfinni fylgja tilkynningunni.

Sjá nánar 33. gr. pvrg.

3. Hvenær telst ábyrgðaraðili hafa orðið var við öryggisbrot?

Ábyrgðaraðili telst hafa orðið var við öryggisbrot þegar hann hefur **ákveðna vissu (e. reasonable degree of certainty)** fyrir því að öryggisbrot hafi átt sér stað sem leitt hefur til þess að persónuupplýsingar voru í hættu. Þetta fer eftir aðstæðum hverju sinni. Í sumum tilvikum er nokkuð skýrt að um brot hafi verið að ræða, á meðan í öðrum tilvikum kann að taka tíma að staðfesta hvort persónuupplýsingar hafi komist í hættu.

Áhersla skal vera á skjót viðbrögð við að rannsaka tilvikið til að ákvarða hvort öryggisbrot hafi átt sér stað, og ef svo er, að gera viðeigandi ráðstafanir og tilkynna til Persónuverndar/einstaklinga ef þörf krefur.

Dæmi
Þegar geisladiskur tapast með ódulkóðuðum gögnum er oft ekki mögulegt að staðfesta hvort utanaðkomandi aðili hafi komist í gögnin. Aftur á móti er nauðsynlegt að tilkynna um slíkt brot þar sem til staðar er ákveðin vissa (reasonable degree of certainty) fyrir því að brot hafi átt sér stað, sem ábyrgðaraðilinn varð var við þegar hann uppgötvaði að geisladiskurinn hefði tapast.

Dæmi
Þegar þriðji aðili upplýsir ábyrgðaraðila um að hann hafi fyrir mistök móttekið persónuupplýsingar um viðskiptavin hans og leggur fram gögn því til stuðnings að miðlunin hafi verið óheimil. Þar sem

ábyrgðaraðilinn hefur verið upplýstur um að brot hafi átt sér stað er ekki nokkur vafi á að hann teljist hafa orðið var við brotið.

Dæmi
Þegar ábyrgðaraðili kemst að því að hugsanlega hafi verið brotist inn í kerfin hans. Ábyrgðaraðilinn kannar kerfin til að sannreyna hvort persónuupplýsingar hafi verið í hættu og staðfestir að svo sé. Þarna hefur ábyrgðaraðilinn sönnun fyrir því að brot hafi átt sér stað og því er enginn vafi á því að hann hafi orðið var við brotið.

Þegar ábyrgðaraðili fær fyrst upplýsingar um mögulegt öryggisbrot frá einstaklingi, fyrirtæki eða þegar hann uppgötvar það sjálfur, hefur hann **ákveðið svigrúm í stuttan tíma til að komast að því hvort um brot hafi í raun verið að ræða.** Á meðan á þessu rannsóknartímabili stendur er ekki talið að ábyrgðaraðili hafi „orðið var við“ öryggisbrot.

Nauðsynlegt er að í þessum fyrstu viðbrögðum ábyrgðaraðila felist einnig **mat á líkum á áhættu fyrir einstaklinga** í tengslum við mat á því hvort nauðsynlegt sé að upplýsa einstaklingana um brotið.

Dæmi

Einstaklingur upplýsir ábyrgðaraðila um að hann hafi móttekið tölvupóst, að því er virðist frá ábyrgðaraðilanum, sem hafi innihaldið persónuupplýsingar sem tengdust raunverulegum notum hans á þjónustu ábyrgðaraðilans. Einstaklingurinn bendir einnig á að svo virðist sem um öryggisbrot hafi verið að ræða hjá ábyrgðaraðilanum. Ábyrgðaraðilinn framkvæmir rannsókn á stuttum tíma og kemur auga á öryggisbrot sem hefur orðið í kerfinu og vísbendingu um óheimilan aðgang að persónuupplýsingum. Á þeim tímapunkti væri ábyrgðaraðilinn talinn hafa orðið var við öryggisbrotið og væri honum þá nauðsynlegt að tilkynna til Persónuverndar að öryggisbrot hefði orðið ef það felur í sér áhættu fyrir einstaklinga. Þá þarf ábyrgðaraðilinn þarf einnig að gera viðeigandi ráðstafanir vegna atviksins.

Til að ábyrgðaraðili geti komið auga á og brugðist við öryggisbrotum ættu að vera til staðar **innri verkferlar** hjá honum. Þegar upp kemst um öryggisbrot er mikilvægt er að viðeigandi aðilar innan fyrirtækis séu upplýstir, þannig að unnt sé að bregðast við með viðeigandi hætti eftir því sem þörf er á.

Ábyrgðaraðilinn ætti einnig að koma upp sérstöku fyrirkomulagi þegar kemur að skyldu vinnsluaðila til að upplýsa ábyrgðaraðila um öryggisbrot.

Þó það sé á ábyrgð ábyrgðaraðila og vinnsluaðila að gera **viðeigandi ráðstafanir til að koma í veg fyrir og bregðast við öryggisbrotum** eru hér nokkur skref sem alltaf skal fylgja þegar uppi er grunur um öryggisbrot:

- Upplýsingum varðandi atburði sem tengjast öryggismálum skal beint til tiltekinna einstaklinga, sem bera ábyrgð á viðbrögðum við öryggisbrotum, staðfestingu á hvort um öryggisbrot hafi verið að ræða og mati á áhættu.
- Því næst skal meta áhættu fyrir einstaklinga í kjölfar öryggisbrots (líkur á engri áhættu, áhættu eða mikilli áhættu), auk þess sem viðeigandi aðilar innan fyrirtækisins skulu upplýstir.
- Tilkynning send til Persónuverndar og hugsanleg tilkynning til þeirra einstaklinga sem öryggisbrotið hefur áhrif á, ef þörf krefur.

- Á meðan á þessu öllu stendur skal ábyrgðaraðili framkvæma þær ráðstafanir sem þarf til að takmarka tjón.

Ábyrgðaraðila er skylt að bregðast við upphaflegri tilkynningu um hugsanlegt öryggisbrot og komast að því hvort um brot var að ræða. Þegar ábyrgðaraðili hefur komist að því að líkur eru á að um öryggisbrot hafi verið að ræða, þá þarf hann **að tilkynna Persónuvernd þar um eigi síðar en 72 klst. síðar.** Litið verður svo á að skilyrði 33. gr. persónuverndarreglugerðarinnar hafi ekki verið uppfyllt ef ábyrgðaraðili bregst ekki tímanlega við með tilkynningu og ljóst verður að öryggisbrot hafi átt sér stað.

Það að ábyrgðaraðili hafi virka verkferla til að koma upp um og takast á við öryggisbrot, sem og að tilkynna um þau, er einnig nauðsynlegur hluti af viðeigandi tæknilegum og skipulagslegum öryggisráðstöfunum sem honum er skylt að framkvæma skv. 32. gr. reglugerðarinnar.

4. Hverjar eru skyldur vinnsluaðila?

Það er ábyrgðaraðili sem ber fyrst og fremst ábyrgð á öryggi persónuupplýsinga, en vinnsluaðili hefur einnig mikilvægu hlutverki að gegna til að tryggja að ábyrgðaraðili geti uppfyllt skyldur sínar, m.a. hvað varðar tilkynningar um öryggisbrot. Samningur við vinnsluaðila skv. 28. gr. reglugerðarinnar[1] skal m.a. kveða á um að vinnsluaðili aðstoði ábyrgðaraðila við að tryggja að skyldur hans hvað varðar tilkynningu um öryggisbrot séu uppfylltar, að teknu tilliti til eðlis vinnslunnar og upplýsinga sem vinnsluaðili hefur aðgang að.

Vinnsluaðili skal tilkynna ábyrgðaraðila um það ***án ótilhlýðilegrar tafar*** ef hann verður var við öryggisbrot í tengslum við vinnslu persónuupplýsinga. Hér þarf að hafa í huga að vinnsluaðilinn þarf ekki að meta líkur á áhættu fyrir einstaklinganna áður en hann tilkynnir ábyrgðaraðila, hann þarf eingöngu að staðfesta að brot hafi orðið og tilkynna það ábyrgðaraðila. Litið er svo á að ábyrgðaraðili hafi orðið var við brot þegar vinnsluaðili tilkynnir honum um það.

Mælt er með því að vinnsluaðili tilkynni ábyrgðaraðila umsvifalaust um brotið og veiti honum frekari upplýsingar um það um leið og þær verða tiltækar. Þetta er mikilvægt til að tryggja að ábyrgðaraðili geti brugðist við innan 72 klst. tímarammans og tilkynnt Persónuvernd.

Ef vinnsluaðili þjónustar fleiri en einn ábyrgðaraðila sem allir verða fyrir sama öryggisbroti skal hann veita hverjum og einum ábyrgðaraðila upplýsingar um atvikið.

Ábyrgðaraðili getur falið vinnsluaðila að senda tilkynningu fyrir sína hönd en slíkt þarf að mæla fyrir um í vinnslusamningi, sbr. 28. gr. pvrg. Mikilvægt er að hafa í huga að hin lagaleg ábyrgð hvílir þó áfram á ábyrgðaraðilanum.

Sjá 3. mgr. 28. gr. 33. gr. og 34. gr. pvrg. svo og leiðbeiningar Persónuverndar fyrirvinnsluaðila.

5. Hvaða upplýsingar er skylt að veita Persónuvernd?

Þegar ábyrgðaraðili tilkynnir um öryggisbrot til Persónuverndar skal í tilkynningunni[2] a.m.k.:

a) lýsa eðli öryggisbrots við meðferð persónuupplýsinga, þ.m.t., ef hægt er, þeim flokkum og áætluðum fjölda skráðra einstaklinga sem það varðar og flokkum og áætluðum fjölda skráninga persónuupplýsinga sem um er að ræða,

[1] Sjá nánar leiðbeiningar til vinnsluaðila á vefsíðu Persónuverndar. Þar er m.a. að finna fyrirmynd að ákvæði sem þessu.
[2] Ath. að fyrirhugað er að Persónuvernd bjóði upp á rafrænt tilkynningareyðublað á vefsíðu sinni sem ábyrgðaraðilar munu geta notað til að senda inn tilkynningar um öryggisbrot.

b) gefa upp nafn og samskiptaupplýsingar persónuverndarfulltrúa eða annars tengiliðar þar sem hægt er að fá frekari upplýsingar,
c) lýsa líklegum afleiðingum öryggisbrots við meðferð persónuupplýsinga,
d) lýsa þeim ráðstöfunum sem ábyrgðaraðili hefur gert eða fyrirhugar að gera vegna öryggisbrots við meðferð persónuupplýsinga, þ.m.t., eftir því sem við á, ráðstöfunum til að milda hugsanleg skaðleg áhrif þess.

Þó að ekki liggi allar upplýsingar fyrir, svo sem nákvæmur fjöldi einstaklinga sem brotið hefur áhrif á, skal það ekki koma í veg fyrir að tilkynning sé send tímanlega inn. Áætla má fjölda einstaklinga sem og fjölda skráa sem brotið hefur áhrif á. Þegar fyrir liggur að öryggisbrot hefur átt sér stað, en umfang þess er ekki enn þekkt, er tilkynning í áföngum kjörin leið til að uppfylla kröfur um tilkynningu.

Framangreind upptalning á þeim upplýsingum sem fram skulu koma í tilkynningum um brot er ekki tæmandi. Er ábyrgðaraðila því frjálst að veita frekari upplýsingar, kjósi hann svo, en það kann t.d. að ráðast af eðli brots sem um ræðir. Ábyrgðaraðila gæti einnig þótt gagnlegt að tilgreina vinnsluaðila, ef rót brotsins má rekja til hans.

Í öllum tilvikum kann Persónuvernd að óska eftir frekari upplýsingum í tengslum við rannsókn sína á brotinu.

Sjá 3. mgr. 33. gr. pvrg.

6. Þarf tilkynning til Persónuverndar að innihalda allar upplýsingar um öryggisbrot?

Nei. Frekari rannsókn ábyrgðaraðila kann að vera nauðsynleg til að staðreyna allar þær upplýsingar sem máli skipta, en þetta fer eftir eðli öryggisbrotsins hverju sinni. Vegna þessa er heimilt að veita upplýsingar um öryggisbrot í áföngum án ástæðulausrar tafar, svo fremi sem gefnar eru upp ástæður fyrir þessum töfum.

Líklegt er að þetta verði raunin vegna flóknari öryggisbrota, s.s. varðandi tölvuglæpi þar sem nákvæm rannsókn kann að vera nauðsynleg til að staðreyna fyllilega eðli brotsins og að hve miklu leyti persónuupplýsingum hefur verið ógnað.

Hafa skal í huga að eftir að upphafleg tilkynning hefur verið send til Persónuverndar getur ábyrgðaraðili sent uppfærðar upplýsingar, ef frekari rannsókn sýnir fram á að ekkert öryggisbrot hafi í raun átt sér stað. Þessum upplýsingum væri þá bætt við þær upplýsingar sem þegar hefðu verið veittar, og atvikið skráð í framhaldinu sem atvik sem ekki fól í sér brot. **Engin viðurlög eru við því að tilkynna um brot sem síðar kemur í ljós að var í reynd ekki brot.**

Dæmi

Ábyrgðaraðili tilkynnir Persónuvernd innan 72 klst. frá því að upp kemst um öryggisbrot þar sem geisladiskur týnist, sem innihélt afrit af persónuupplýsingum viðskiptavina hans. Geisladiskurinn finnst síðar, þar sem hann hafði einfaldlega verið geymdur á röngum stað innan fyrirtækisins. Ábyrgðaraðilinn sendir Persónuvernd uppfærðar upplýsingar og óskar eftir því að tilkynningunni verði breytt.

7 Öryggisbrot sem hafa áhrif á einstaklinga í fleiri en einu aðildarríki

Þegar vinnsla persónuupplýsinga fer fram yfir landamæri getur öryggisbrot haft áhrif á skráða einstaklinga í fleiri en einu aðildarríki. Í 1. mgr. 33. gr. pvrg. kemur fram að ábyrgðaraðili skuli

tilkynna til þess eftirlitsyfirvalds sem lögbært er skv. 55. gr. reglugerðarinnar. Í þessu felst að þegar brot hefur áhrif á persónuupplýsingar einstaklinga í fleiri en einu aðildarríki og nauðsynlegt er að tilkynna um það, þarf ábyrgðaraðilinn að **tilkynna forystueftirlitsyfirvaldinu (e. lead supervisory authority)** um öryggisbrotið.

Þegar ábyrgðaraðili leggur drög að viðbragðsáætlun sinni vegna öryggisbrota þarf hann að framkvæma mat á því hvaða eftirlitsyfirvald er forystueftirlitsyfirvald hans, sem senda þarf tilkynningar til. Þá getur ábyrgðaraðili brugðist skjótt við broti og uppfyllt skyldur sínar samkvæmt 33. gr.

Sé ábyrgðaraðili í vafa um hvert forystueftirlitsyfirvaldið er ætti viðkomandi að minnsta kosti að tilkynna um brot til þess eftirlitsyfirvalds þar sem brotið átti sér stað.

Sjá nánar 33., 55. og 56. gr. pvrg.

8. Í hvaða tilvikum þarf ekki að senda Persónuvernd tilkynningu um öryggisbrot?

Ekki þarf að tilkynna Persónuvernd um brot sem **ólíklegt þykir að leiði til áhættu fyrir réttindi og frelsi einstaklinga**. Sem dæmi um slík brot má nefna þegar persónuupplýsingar eru þegar opinberar og miðlun slíkra gagna er ekki líkleg til að skapa áhættu fyrir einstaklinginn.

Dæmi

Dæmi um öryggisbrot sem ekki þarf að tilkynna um væri tap á búnaði, sem er örugglega dulkóðaður. Svo fremi sem dulkóðunarlykillinn væri tryggilega varðveittur og þetta væri ekki ekki eina eintakið af persónuupplýsingunum, þá væru persónuupplýsingarnar í þessu tilviki óaðgengilegar fyrir utanaðkomandi. Er því brotið ólíklegt til að leiða til áhættu fyrir réttindi og frelsi hinna skráðu í þessu tilviki. Komi síðar í ljós að dulkóðunarlykillinn var óöruggur, þá væri áhætta til staðar og kynni þá tilkynningar að vera þörf.

9. Hvenær þarf að upplýsa einstaklinga?

Ekki þarf að upplýsa einstaklinga um öll öryggisbrot.

Ef líklegt er að öryggisbrot við meðferð persónuupplýsinga leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklinga skal ábyrgðaraðili tilkynna hinum skráða um brotið án ótilhlýðilegrar tafar.

Er því hærri þröskuldur fyrir því hvenær þarf að upplýsa einstaklinga heldur en Persónuvernd.

Megintilgangur þessarar tilkynningar er að veita upplýsingar um þau úrræði sem einstaklingar geta sjálfir gripið til til þess að vernda sig, svo sem að setja ný lykilorð.

10. Hvaða upplýsingar er skylt að veita einstaklingum?

Hér gilda sömu reglur og varðandi tilkynningar til Persónuverndar.

Samkvæmt því skal ábyrgðaraðili að minnsta kosti veita eftirfarandi upplýsingar:

- lýsingu á eðli öryggisbrotsins;
- nafn og samskiptaupplýsingar persónuverndarfulltrúa eða annars tengiliðar;
- lýsingu á líklegum afleiðingum öryggisbrotsins; og

- lýsingu á þeim ráðstöfunum sem ábyrgðaraðili hefur gert eða fyrirhugar að gera vegna öryggisbrotsins, þar á meðal, þar sem við á, ráðstöfunum til að milda hugsanleg skaðleg áhrif.

Varðandi ráðstafanir sem gerðar hafa verið gæti ábyrgðaraðili t.d. tekið fram að eftir að hafa tilkynnt um öryggisbrotið til Persónuverndar hafi hann fengið ráðgjöf um hvernig draga mætti úr áhrifum þess. Ábyrgðaraðilinn ætti einnig, þar sem við á, að veita einstaklingunum nákvæmar ráðleggingar um hvernig þeir geta varið sig fyrir hugsanlegum skaðlegum áhrifum öryggisbrotsins, svo sem með því að skipta um lykilorð. Ekki er um tæmandi talningu að ræða, og getur ábyrgðaraðili því valið að veita frekari upplýsingar.

Sjá 34. gr. pvrg. og væntanlegar leiðbeiningar Persónuverndar um gagnsæi.

11. Hvernig skal hafa samband við einstaklinga?

Nota skal sérstaka tilkynningu þegar einstaklingar eru upplýstir um öryggisbrot og er því til dæmis ekki heimilt að senda slíka tilkynningu með öðrum upplýsingum, s.s. fréttabréfum. Eykur þetta skýrleika og gagnsæi.

Dæmi um gagnsæjar samskiptaleiðir eru tölvupóstur eða smáskilaboð, áberandi upplýsingar á heimasíðu, samskipti með pósti eða áberandi auglýsingar í prentmiðlum. Mælt er með því að ábyrgðaraðili velji aðferð sem eykur líkurnar á því að upplýsingarnar komist til hinna skráðu. Ábyrgðaraðili kann því að velja að nota nokkrar aðferðir.

Ábyrgðaraðili kann einnig að þurfa að taka tillit til þess að tilkynningar séu aðgengilegar í ólíkum útgáfum, svo sem á viðeigandi tungumálum, til að tryggja að hinir skráðu skilji upplýsingarnar.

Ábyrgðaraðilar eru best til þess fallnir að meta viðeigandi samskiptamáta við hina skráðu, sér í lagi ef þeir eiga í reglulegum samskiptum við viðskiptavini sína. Aftur á móti þarf ábyrgðaraðili að hafa varann á þegar notaðar eru samskiptaleiðir sem hafa orðið fyrir viðkomandi öryggisbroti. Ábyrgðaraðilar kunna því að vilja leita ráðgjafar Persónuverndar, ekki eingöngu um efni tilkynningar heldur einnig varðandi hentuga samskiptamáta við einstaklinga.

Sjá 2. mgr. 34. gr. pvrg. svo og væntanlegar leiðbeiningar Persónuverndar um gagnsæi.

12. Hvenær þarf ekki að upplýsa einstaklinga?

Ef ábyrgðaraðili getur sýnt fram á að eitt eða fleiri eftirfarandi skilyrða séu uppfyllt þarf ekki að gera einstaklingi viðvart um öryggisbrot:

- Ábyrgðaraðilinn hefur gert viðeigandi tæknilegar og skipulagslegar verndarráðstafanir og þessar ráðstafanir voru gerðar varðandi þær persónuupplýsingar sem öryggisbrotið hafði áhrif á. Hér er einkum átt við ráðstafanir til að gera persónuupplýsingar ólæsilegar hverjum þeim sem ekki hefur aðgangsheimild að þeim, s.s. með dulkóðun.
- Ábyrgðaraðilinn hefur gert ráðstafanir strax í kjölfar öryggisbrotsins til þess að útiloka þá áhættu sem skapaðist í kjölfar þess, til dæmis með því að grípa til aðgerða gagnvart einstaklingi sem hefur fengið aðgang að persónuupplýsingum án heimildar áður en hann gat gert eitthvað við þær.
- Það hefur í för með sér óhóflega fyrirhöfn að tilkynna einstaklingunum um öryggisbrotið. Í því tilviki skal í staðinn birta almenna tilkynningu eða grípa til svipaðrar ráðstöfunar þar sem hinum skráðu er gert viðvart með jafnáhrifaríkum hætti.

13. Hvaða atriði þarf að hafa í huga við mat á áhættu?

Ekki þarf að tilkynna um öryggisbrot í öllum tilvikum:

- Tilkynning til Persónuverndar er eingöngu nauðsynleg þegar líklegt er talið að öryggisbrotið leiði af sér áhættu fyrir réttindi og frelsi einstaklings.
- Tilkynning til einstaklinga eru eingöngu nauðsynleg þegar líklegt er að öryggisbrot leiði af sér mikla áhættu fyrir réttindi og frelsi þeirra.

Þetta felur í sér að um leið og ábyrgðaraðili verður var við öryggisbrot er afar mikilvægt að hann bæði leiti leiða til að takmarka tjónið og leggi mat á þá áhættu sem öryggisbrotið kann að leiða af sér.

Þegar áhrif áhættu fyrir einstaklinga í kjölfar öryggisbrots eru metin ætti matið að taka tillit til eftirfarandi atriða:

- **Tegund öryggisbrots**
  - Tegund öryggisbrots getur skipt máli. Miðlun heilsufarsupplýsinga til utanaðkomandi aðila (e. Confidentiality Breach) kann til dæmis að hafa aðrar afleiðingar en þegar slíkar upplýsingar glatast (e. Availability Breach.)
- **Eðli, viðkvæmni og magn persónuupplýsinga**
  - Almennt séð er áhættan þeim mun meiri eftir því sem persónuupplýsingarnar eru viðkvæmari. Þá er miðlun upplýsinga sem þegar eru opinberar, svo sem nafn og heimilisfang, yfirleitt talin ólíkleg til að leiða til verulegs tjóns. Sé nafni og heimilisfangi foreldra sem hafa ættleitt barn aftur á móti miðlað til líffræðilegrar móður barnsins geta afleiðingarnar verið alvarlegar, bæði fyrir einstaklingana sem ættleiddu barnið og barnið sjálft. Einnig geta brot sem varða heilsufarsupplýsingar eða fjárhagsupplýsingar valdið tjóni eða leitt til þess að upplýsingarnar verði notaðar til auðkennaþjófnaðar. Þá er áhættan yfirleitt meiri þegar um er að ræða blöndu persónuupplýsinga, s.s. bæði fjárhags- og heilsufarsupplýsingar, fremur en eina tegund upplýsinga. Að lokum getur öryggisbrot sem varðar lítið magn mjög viðkvæmra persónuupplýsinga haft mikil áhrif á einstakling.
- **Hversu auðvelt er að persónugreina einstaklingana?**
  - Auðkenning kann að vera möguleg á grundvelli persónuupplýsinganna einna og sér, án frekari aðgerða. Í öðrum tilvikum getur verið mjög erfitt að tengja viðkomandi persónuupplýsingar við tiltekinn einstakling, en þó mögulegt. Þetta getur skipt máli.
- **Alvarleiki áhrifanna fyrir einstaklinga**
  - Sá skaði sem öryggisbrot hefur í för með sér fyrir einstaklinga getur verið sérlega mikill í sumum tilvikum (til dæmis þegar um er að ræða viðkvæmar persónuupplýsingar), sérstaklega þegar öryggisbrot getur leitt til auðkennisþjófnaðar eða svika, líkamlegs skaða, mikils andlegs álags, niðurlægingar eða orðsporsmissis.
- **Sérstakt eðli einstaklinganna**
  - Öryggisbrot getur varðað persónuupplýsingar um börn eða aðra viðkvæma hópa einstaklinga, sem eru í meiri áhættu fyrir vikið.
- **Fjöldi þeirra einstaklinga sem verða fyrir öryggisbrotinu**
  - Almennt hefur öryggisbrot meiri áhrif eftir því sem fleiri einstaklingar verða fyrir áhrifum.
- **Sérstakt eðli ábyrgðaraðilans**

- Eðli og hlutverk ábyrgðaraðilans og starfsemi hans kann að hafa áhrif á áhættumatið. Til dæmis er meiri áhætta ef læknastofa verður fyrir öryggisbroti, borið saman við netfangalista dagblaðs.

- **Almenn atriði**
  - Ábyrgðaraðili þarf að meta heildstætt ýmis atriði við mat á þeirri áhættu sem kann að leiða af öryggisbroti fyrir réttindi og frelsi einstaklinga.

14. Skrá yfir öryggisbrot

Ábyrgðaraðili skal skrá niður hvers kyns öryggisbrot sem verða við vinnslu persónuupplýsinga og tilgreina málsatvik í tengslum við viðkomandi brot, áhrif þess og þær aðgerðir til úrbóta sem gripið var til.

Þá er mælt með því að ábyrgðaraðili skrái einnig rök fyrir ákvarðanatöku þegar öryggisbrot á sér stað og þeim ráðstöfunum sem gerðar eru. Slík skráning aðstoðar til dæmis í samskiptum við Persónuvernd, ef tilkynning berst of seint.

Dæmi um öryggisbrot og hverjum þarf að gera viðvart:

Dæmi	Tilkynning til Persónuverndar?	Tilkynning til einstaklings?	Athuga
i. Ábyrgðaraðili varðveitti afrit af gögnum, sem innihéldu persónuupplýsingar, á geisladiski, en upplýsingarnar voru dulkóðaðar. Geisladisknum er stolið í innbroti.	Nei.	Nei.	Svo lengi sem gögnin eru dulkóðuð með aðferð sem byggir á nýjustu tækni, t.d. með algrími, og til eru önnur afrit af gögnunum, og afritunarlykillinn er ekki í hættu, kann þetta ekki að vera brot sem þarf að tilkynna um.
ii. Ábyrgðaraðili heldur úti þjónustu á netinu. Í kjölfar netárásar á þjónustuna eru persónuupplýsingar einstaklinga gerðar aðgengilegar, Viðskiptavinir ábyrgðaraðilans eru allir staðsettir í einu aðildarríki.	Já, þegar það er líklegt að brotið hafi einhverjar afleiðingar fyrir einstaklinganna í ljósi þess að hér er um að ræða öryggisbrot sem veldur því að persónuupplýsingar verða óaðgengilegar.	Já, en fer eftir eðli persónupplýsinganna sem um er að ræða og alvarleika áhættunnar fyrir einstaklingana.	Ef áhættan er ekki mjög mikil, þá er mælt með því að upplýsa hina skráðu – en það fer þó eftir eðli aðstæðnanna. Til dæmis kann tilkynningar ekki að vera þörf þegar um er að ræða öryggisbrot varðandi fréttabréf um sjónvarpsþætti, en tilkynningar kann að vera þörf ef þetta fréttabréf getur leitt til þess að pólitísk skoðun hins skráða er gerð opinber.
iii. Rafmagnsleysi stendur yfir í	Nei.	Nei.	Þótt ekki þurfi að tilkynna um brotið þarf

nokkrar mínútur í þjónustuveri, sem felur í sér að viðskiptavinir geta ekki hringt í ábyrgðaraðila og fengið aðgang að gögnunum sínum.			engu að síður að skrá það í skrá um öryggisbrot.
iv. Tölvuárás er gerð á ábyrgðaraðila, sem leiðir til þess að öll gögn hans eru dulkóðuð. Um einu eintökin af gögnunum er að ræða, sem nú eru óaðgengileg. Við rannsókn kemur í ljós að einu afleiðingar árásarinnar eru umrædd dulkóðun.	Já.	Já, en fer eftir eðli persónupplýsinganna sem um er að ræða og alvarleika áhættunnar fyrir einstaklingana.	Ef til staðar hefði verið annað eintak af gögnunum, og hægt hefði verið að endurheimta þau innan skamms tíma, hefði ekki verið nauðsynlegt að tilkynna um þetta atvik til Persónuverndar eða hinna skráðu einstaklinga, þar sem ekki hefði verið um að ræða skort á aðgengi. Persónuvernd kann aftur á móti að taka til skoðunar að rannsaka atvikið til að kanna eftirfylgni með öryggiskröfum.
v. Einstaklingur hringir í þjónustuver banka til að tilkynna öryggisbrot. Hann hefur fengið mánaðaryfirlit fyrir annan einstakling. Ábyrgðaraðilinn framkvæmir stutta rannsókn (lokið innan 24 klst.) og ákvarðar með nokkurri vissu að um öryggisbrot hafi verið að ræða, og ef um er að ræða kerfisvillu, hvort hún getur hafa haft áhrif á aðra einstaklinga.	Já.	Einstaklingarnir, sem brotið hafði áhrif á, eru eingöngu látnir vita ef um er að ræða mikla áhættu.	Ef ljóst er, eftir frekari rannsókn, að brotið hafði áhrif á fleiri einstaklinga þarf að upplýsa Persónuvernd um það, og ábyrgðaraðilinn þarf að sjá til þess að aðrir einstaklingar séu látnir vita, ef um er að ræða mikla áhættu.

vi. Fjölþjóðleg netverslun verður fyrir tölvuárás, og notendanöfn, lykilorð og kaupsaga viðskiptavina eru í kjölfarið birt á Netinu.	Já, tilkynna forystueftirlits-yfirvaldi, ef um er að ræða vinnslu sem fer yfir landamæri.	Já, þar sem atvikið getur leitt til mikillar áhættu.	Ábyrgðaraðilinn ætti að grípa til ráðstafana, m.a. með því að tryggja að þeir viðskiptavinir, sem um ræðir, skipti um lykilorð.
vii. Fyrirtæki sem hýsir vefsíður (vinnsluaðili) kemur auga á villu í hugbúnaðnum, sem stýrir aðgangsheimildum. Afleiðingarnar eru þær að hvaða notandi sem er getur komist inn í upplýsingar annars notanda.	Sem vinnsluaðili verður fyrirtækið að hafa samband við viðskiptavinina sem um ræðir (ábyrgðaraðilana.) Ef gert er ráð fyrir því að vinnsluaðilinn hafi framkvæmt sína eigin rannsókn ættu ábyrgðaraðilarnir sem um ræðir að vera nokkuð vissir um hvort öryggisbrot hafi átt sér stað, og ættu þannig að hafa orðið varir við brot þegar þeir hafa fengið tilkynninguna frá vinnsluaðilanum. Því næst skulu ábyrgðaraðilarnir upplýsa Persónuvernd um brotið.	Ef líklega var ekki um mikla áhættu að ræða fyrir einstaklinga þarf ekki að gera þeim viðvart.	Fyrirtækið sem hýsir vefsíðurnar (vinnslu-aðilinn) verður að meta hvort nauðsynlegt sé að gera öðrum viðvart á öðrum grundvelli, sbr. t.d. NIS-tilskipunina (tilskipun ESB um net- og upplýsingaöryggi, nr. 2016/1148/EU).
viii. Sjúkraskýrslur á spítala eru óaðgengilegar í 30 klst. vegna netárásar.	Já.	Já.	
ix. Persónuupplýsingar 5000 nemenda eru fyrir mistök sendar á rangan póstlista, með yfir 1000 viðtakendum.	Já.	Já, en fer eftir eðli persónu-upplýsinganna og alvarleika hugsanlegra afleiðinga.	
x. Tölvupóstur með beinni	Já, tilkynning til Persónuverndar	Já, en fer eftir umfangi og eðli	Tilkynning er mögulega ekki nauðsynleg ef engar

markaðssetningu er sendur viðtakendum í „til“ eða „cc“, sem leiðir til þess að aðrir viðtakendur geta séð hina viðtakendur póstsins.	kann að vera nauðsynleg ef um stóran hóp einstaklinga var að ræða, ef viðvkæmar upplýsingar eru gerðar opinberar (s.s. netfangalisti geðlæknis) eða ef aðrir þættir leiða til mikillar áhættu (s.s. ef tölvupósturinn innihélt lykilorð.)	persónu-upplýsinganna.	viðkvæmar upplýsingar voru gerðar opinberar og ef um fáa einstaklinga var að ræða.