**TILKYNNING UM ÖRYGGISBREST**

**skv. 27. gr. laga nr. 90/2018, sbr. 33. gr. pvrg.**

***Tilkynningar um öryggisbrest skulu sendar á netfangið postur@personuvernd.is eða afhentar á skrifstofu Persónuverndar á opnunartíma stofnunarinnar.***

***Athugið að ábyrgðaraðili skal, án ótilhlýðilegrar tafar og, ef mögulegt er, eigi síðar en 72 klst. eftir að hann verður brestsins var, tilkynna um hann til Persónuverndar nema ólíklegt þyki að bresturinn leiði til áhættu fyrir réttindi og frelsi einstaklinga, skv. 2. mgr. 27. gr. laga nr. 90/2018, sbr. einnig 1. mgr. 33. gr. persónuverndarreglugerðarinnar.***

*Stjörnumerktum (\*) spurningum er skylt að svara.*

1. **Tilkynnandi** \*

|  |  |  |
| --- | --- | --- |
| **Fyrirtæki / stofnun** | **Kennitala** | **Geiri / tegund starfsemi** |
|  |  |  |

* 1. **Upplýsingar um þann sem getur veitt frekari upplýsingar um öryggisbrestinn**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nafn tengiliðar** | **Staða** | **Netfang** | **Símanúmer** |
|  |  |  |  |

* 1. **Dagsetning og staður tilkynningar um öryggisbrest**

|  |  |
| --- | --- |
| **Dagsetning** | **Staður** |
|  |  |

1. **Dagsetningar og tími öryggisbrests\***
	1. **Dagsetning og tími þegar ábyrgðaraðili varð öryggisbrestsins var:**
	2. **Hefur ábyrgðaraðili upplýsingar um dagsetningu á upphafi og/eða lokum öryggisbrests?**

|  |  |
| --- | --- |
| **❍** | Já |
| **❍** | Nei |

* + 1. **Ef JÁ: Dagsetning og tími á upphafi öryggisbrests:**
		2. **Ef JÁ: Dagsetning og tími á lokum öryggisbrests:**
	1. **Stendur öryggisbresturinn enn yfir?**

|  |  |
| --- | --- |
| **❍** | Já |
| **❍** | Nei |
| **❍** | Ekki vitað |

* 1. **Ef tilkynning berst þegar meira en 72 klst. eru liðnar frá því að vart varð við brotið, vinsamlegast tilgreinið ástæður þess hér:**

|  |
| --- |
| 1. **/ 250**
 |

* 1. **Hvernig varð ábyrgðaraðili var við öryggisbrestinn?**

|  |  |
| --- | --- |
| **𛲠** | Með tæknilegum öryggisráðstöfunum sem eiga sér stað með sjálfvirkum hætti  |
| **𛲠** | Með skipulagslegum ráðstöfunum, t.d. reglubundnum athugunum |
| **𛲠** | Starfsmaður gerði viðvart um öryggisbrestinn |
| **𛲠** | Vinnsluaðili gerði viðvart um öryggisbrestinn |
| **𛲠** | Utanaðkomandi aðili gerði viðvart um öryggisbrestinn |
| **𛲠** | Annað: \_\_\_\_\_\_\_\_\_\_\_\_ |

* 1. **Hvers vegna varð öryggisbresturinn að mati ábyrgðaraðila (þínu mati / þíns fyrirtækis eða stjórnvalds)?**

|  |  |
| --- | --- |
| **𛲠** | Mannleg mistök: einstakt tilvik |
| **𛲠** | Skortur á skipulagslegum ráðstöfunum: kerfisbundið frávik (e. Lack of organisational routines or procedures: systematic errors) |
| **𛲠** | Tæknilegt frávik, t.d. hugbúnaðarvilla eða stillingar forrita (e. software bugs/program settings) |
| **𛲠** | Árásir framkvæmdar af ásetningi af aðila innan fyrirtækis eða stofnunar |
| **𛲠** | Fjandsamleg árás af hálfu utanaðkomandi aðila |
| **𛲠** | Óþekktar ástæður |
| **𛲠** | Annað: \_\_\_\_\_\_\_\_\_\_\_\_ |

1. **Um öryggisbrestinn**
	1. **Lýstu öryggisbrestinum með almennum hætti:\***

|  |
| --- |
| **0 / 250** |

* 1. **Hafa verið borin kennsl á þá aðila sem eru ábyrgir fyrir eða eiga þátt í öryggisbrestinum, ef við á?\***

*Hér er átt við aðila sem hafa valdið öryggisbresti með saknæmum hætti, s.s. ef fyrirtæki hefur orðið fyrir netárás.*

|  |  |
| --- | --- |
| **❍** | Já |
| **❍** | Nei |
| **❍** | Ekki vitað |

* 1. **Hefur ábyrgðaraðili gripið til ráðstafana til að milda skaðleg áhrif öryggisbrestsins? \***

|  |  |
| --- | --- |
| **❍** | Já |
| **❍** | Nei |

* + 1. **Ef JÁ, vinsamlegast greinið nánar frá ráðstöfununum og tilgreinið tímasetningar:**

|  |
| --- |
|  |

* 1. **Hversu alvarleg áhætta stafar af öryggisbrestinum að þínu mati?**

|  |  |
| --- | --- |
| **❍** | Hverfandi áhætta |
| **❍** | Takmörkuð áhætta |
| **❍** | Veruleg áhætta |
| **❍** | Hámarksáhætta |
| **❍** | Óþekkt áhætta |
| **❍** | Annað: \_\_\_\_\_\_\_\_\_\_\_\_ |

* 1. **Eðli öryggisbrestsins \***

*Veljið allt sem á við*

|  |  |
| --- | --- |
| **𛲠** | Spillt kerfi / spillikóði |
| **𛲠** | Álagsárás / óvirkt kerfi / skert virkni |
| **𛲠** | Upplýsingasöfnun |
| **𛲠** | Tilraun til að ná stjórn á kerfi |
| **𛲠** | Stjórn náð á kerfi |
| **𛲠** | Upplýsingaöryggi |
| **𛲠** | Svindl / svik |
| **𛲠** | Ólöglegt og óæskilegt efni |
| **𛲠** | Veikleiki |
| **𛲠** | Annað: \_\_\_\_\_\_\_\_\_\_\_\_ |

1. **Tegund upplýsinga**
	1. **Tegundir upplýsinga sem bresturinn varðar \***Veljið allar tegundir sem eiga við.

|  |  |
| --- | --- |
| **𛲠** | Nöfn, fæðingardagar o.þ.h. |
| **𛲠** | Kennitölur |
| **𛲠** | Upplýsingar um tengiliði |
| **𛲠** | Auðkennisupplýsingar (e. Identification data) |
| **𛲠** | Efnahags- og fjármálaupplýsingar |
| **𛲠** | Opinber skjöl |
| **𛲠** | Upplýsingar um staðsetningar |
| **𛲠** | Lykilorð og notendanöfn |
| **𛲠** | Kortanúmer og / eða reikningsnúmer |
| **𛲠** | Launaupplýsingar |
| **𛲠** | Sakfellingar í refsimálum, refsiverð brot og tengdar öryggisráðstafanir |
| **𛲠** | Upplýsingar um þjóðernislegan uppruna einstaklinga |
| **𛲠** | Stjórnmálaskoðanir |
| **𛲠** | Trúarbrögð eða lífsskoðanir |
| **𛲠** | Stéttarfélagsaðild |
| **𛲠** | Upplýsingar um kynhneigð og kynlíf |
| **𛲠** | Heilsufarsupplýsingar |
| **𛲠** | Erfðafræðilegar upplýsingar |
| **𛲠** | Lífkenni |
| **𛲠** | Ekki enn vitað |
| **𛲠** | Annað: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

1. **Um einstaklinga sem öryggisbresturinn varðar**
	1. **Áætlaður fjöldi einstaklinga sem öryggisbresturinn hefur áhrif á: \***

|  |  |
| --- | --- |
| **❍** | 1 - 10 |
| **❍** | 11 - 50 |
| **❍** | 51 - 100 |
| **❍** | 101 - 500 |
| **❍** | 501 - 1.000 |
| **❍** | 1.001 - 10.000 |
| **❍** | 10.001 - 50.000 |
| **❍** | Fleiri en 50.000 |
| **❍** | Ekki vitað / upplýsingar liggja ekki fyrir |
| **❍** | Annað \_\_\_\_\_\_\_\_\_\_\_\_ |

* 1. **Hefur einstaklingum sem öryggisbresturinn hefur áhrif á verið gert viðvart? \***

|  |  |
| --- | --- |
| **❍** | Já |
| **❍** | Nei |

* 1. **Áætlaður fjöldi þeirra skráa með persónuupplýsingum sem öryggisbresturinn hefur áhrif á: \***

|  |  |
| --- | --- |
| **❍** | 1 - 10 |
| **❍** | 11 - 100 |
| **❍** | 101 - 1000 |
| **❍** | 1001 - 10.000 |
| **❍** | 10.001 - 100.000 |
| **❍** | 100.001 - 500..000 |
| **❍** | 500.001 - 1.000.000 |
| **❍** | Fleiri en milljón |
| **❍** | Ekki vitað / upplýsingar liggja ekki fyrir |
| **❍** | Annað: \_\_\_\_\_\_\_\_\_\_\_\_ |

* 1. **Flokkar þeirra einstaklinga sem öryggisbresturinn varðar: \***

*Veljið alla flokka sem eiga við*

|  |  |
| --- | --- |
| **𛲠** | Starfsfólk |
| **𛲠** | Notendur |
| **𛲠** | Nemendur |
| **𛲠** | Viðskiptavinir (núverandi, fyrrverandi og mögulegir) |
| **𛲠** | Sjúklingar |
| **𛲠** | Börn |
| **𛲠** | Einstaklingar í viðkvæmri stöðu (e. vulnerable) |
| **𛲠** | Ekki enn vitað |
| **𛲠** | Annað \_\_\_\_\_\_\_\_\_\_\_\_ |

1. **Afleiðingar**
	1. **Hverjar eru líklegar afleiðingar öryggisbrestsins? \****Veljið allar tegundir sem eiga við.*

|  |  |
| --- | --- |
| **𛲠** | Töpuð yfirráð á persónuupplýsingum |
| **𛲠** | Takmarkanir á rétti / réttindum |
| **𛲠** | Mismunun |
| **𛲠** | Auðkenni stolið |
| **𛲠** | Svik |
| **𛲠** | Fjárhagslegt tjón |
| **𛲠** | Ósamþykktur viðsnúningur á gerviauðkenni (e. unauthorised reversal of pseudonymisation) |
| **𛲠** | Orðsporshnekkir |
| **𛲠** | Upplýsingar sem lúta þagnarskyldu verða aðgengilegar óviðkomandi aðilum |
| **𛲠** | Annað |

1. **Aðgerðir / samskipti**
	1. **Hafa þeir einstaklingar sem málið varðar verið upplýstir um það? \***

|  |  |
| --- | --- |
| **❍** | Já |
| **❍** | Nei, en þeir verða upplýstir |
| **❍** | Nei, og þeir verða ekki upplýstir |
| **❍** | Það hefur ekki verið ákveðið að svo stöddu |
| **❍** | Annað: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

* 1. **Ástæður þess að þeir verða ekki upplýstir: \***

*Eingöngu skal svara þessu ef svar við 7.1. er NEI.*

|  |  |
| --- | --- |
| **❍** | Öryggisbresturinn felur ekki í sér mikla áhættu fyrir réttindi og frelsi einstaklinga |
| **❍** | Persónuupplýsingarnar voru dulkóðaðar eða varðar á annan hátt |
| **❍** | Við höfum nú þegar gripið til aðgerða til að koma í veg fyrir áhættuna |
| **❍** | Það myndi hafa í för með sér óhóflega fyrirhöfn. Við höfum í staðinn birt almenna tilkynningu. |
| **❍** | Hér er um að ræða viðbótarupplýsingar við upphaflega tilkynningu |
| **❍** | Annað |

* 1. **Dagsetning á upplýsingagjöf ef þeir hafa nú þegar verið upplýstir:**
	2. **Áætluð dagsetning ef þeir hafa ekki nú þegar verið upplýstir:**
	3. **Nánari upplýsingar um hvernig einstaklingar hafa verið upplýstir:**

*Ef JÁ - stutt textabox*

|  |
| --- |
|  |

1. **Vinnsla yfir landamæri og aðrar tilkynningar**
	1. **Er fyrirtækið með starfsemi í öðrum löndum? \***

|  |  |
| --- | --- |
| **❍** | Já |
| **❍** | Nei |

*Ef svarið er nei er ekki þörf á að svara fleiri spurningum í þessum kafla.*

* + 1. **Er tilkynningin send til Persónuverndar sem forystustjórnvalds (e. lead supervisory authority) vegna öryggisbrests sem nær yfir landamæri? \***

|  |  |
| --- | --- |
| **❍** | Já |
| **❍** | Nei |
| **❍** | Ekki vitað |

* + 1. **Listi yfir lönd á EES-svæðinu sem öryggisbresturinn snertir:**

*Veljið öll lönd sem eiga við.*

|  |  |
| --- | --- |
| **𛲠** | Austurríki |
| **𛲠** | Belgía |
| **𛲠** | Bretland |
| **𛲠** | Búlgaría |
| **𛲠** | Danmörk |
| **𛲠** | Eistland |
| **𛲠** | Finnland |
| **𛲠** | Frakkland |
| **𛲠** | Grikkland |
| **𛲠** | Holland |
| **𛲠** | Írland |
| **𛲠** | Ítalía |
| **𛲠** | Króatía |
| **𛲠** | Kýpur |
| **𛲠** | Lettland |
| **𛲠** | Liechtenstein |
| **𛲠** | Litháen |
| **𛲠** | Lúxemborg |
| **𛲠** | Malta |
| **𛲠** | Noregur |
| **𛲠** | Portúgal |
| **𛲠** | Pólland |
| **𛲠** | Rúmenía |
| **𛲠** | Slóvakía |
| **𛲠** | Slóvenía |
| **𛲠** | Spánn |
| **𛲠** | Svíþjóð |
| **𛲠** | Tékkland |
| **𛲠** | Ungverjaland |
| **𛲠** | Þýskaland |
| **𛲠** | Ekki vitað |