Kunsill
tal-Unjoni Ewropea

Brussell, 18 ta' Lulju 2022
(OR. en)

11468/22
ADD 1

AVIATION 171
DELACT 120

NOTA TA' TRAŻMISSJONI

minn:	Is-Segretarju Ġenerali tal-Kummissjoni Ewropea, iffirmata mis-Sa Martine DEPREZ, Direttur
data meta waslet:	14 ta' Lulju 2022
lil:	Segretarjat Ġenerali tal-Kunsill
Nru dok. Cion:	C(2022) 4882 final - ANNEX
Suġġett:	ANNESS tar- REGOLAMENT DELEGAT TAL-KUMMISSJONI li jistabbilixxi regoli għall-applikazzjoni tar-Regolament (UE) 2018/1139 tal-Parlament Ewropew u tal-Kunsill, fir-rigward tar-rekwiżiti għall-ġestjoni tar-riskji għas-sigurtà tal-informazzjoni b'impatt potenzjali fuq is-sikurezza tal-avjazzjoni għall-organizzazzjonijiet koperti bir-Regolamenti tal-Kummissjoni (UE) Nru 748/2012 u Nru 139/2014 u li jemenda r-Regolamenti tal-Kummissjoni (UE) Nru 748/2012 u Nru 139/2014

Id-delegazzjonijiet isibu mehmuż id-dokument C(2022) 4882 final - ANNEX.

Mehmuż: C(2022) 4882 final - ANNEX

IL-KUMMISSJONI
EWROPEA

Brussell, 14.7.2022
C(2022) 4882 final

ANNEX

ANNESS

tar-

REGOLAMENT DELEGAT TAL-KUMMISSJONI

li jistabbilixxi regoli għall-applikazzjoni tar-Regolament (UE) 2018/1139 tal-Parlament Ewropew u tal-Kunsill, fir-rigward tar-rekwiżiti għall-ġestjoni tar-riskji għas-sigurtà tal-informazzjoni b'impatt potenzjali fuq is-sikurezza tal-avjazzjoni għall-organizzazzjonijiet koperti bir-Regolamenti tal-Kummissjoni (UE) Nru 748/2012 u Nru 139/2014 u li jemenda r-Regolamenti tal-Kummissjoni (UE) Nru 748/2012 u Nru 139/2014

ANNESS

SIGURTÀ TAL-INFORMAZZJONI — REKWIŻITI TAL-ORGANIZZAZZJONI

[PART-IS.D.OR]

IS.D.OR.100 Kamp ta’ applikazzjoni

Din il-Parti tistabbilixxi r-rekwiżiti li għandhom jiġu ssodisfati mill-organizzazzjonijiet imsemmija fl-Artikolu 2 ta’ dan ir-Regolament.

IS.D.OR.200 Sistema ta’ ġestjoni tas-sigurtà tal-informazzjoni (ISMS)

(a) Sabiex jintlaħqu l-objettivi stabbiliti fl-Artikolu 1, l-organizzazzjoni għandha tistabbilixxi, timplimenta u żżomm sistema ta’ ġestjoni tas-sigurtà tal-informazzjoni (ISMS) li tiżgura li l-organizzazzjoni:

(1) tistabbilixxi politika dwar is-sigurtà tal-informazzjoni li tistabbilixxi l-prinċipji ġenerali tal-organizzazzjoni fir-rigward tal-impatt potenzjali tar-riskji għas-sigurtà tal-informazzjoni fuq is-sikurezza tal-avjazzjoni;

(2) tidentifika u tirrevedi r-riskji għas-sigurtà tal-informazzjoni f’konformità mal-punt IS.D.OR.205;

(3) tiddefinixxi u timplimenta miżuri ta' trattament tar-riskju għas-sigurtà tal-informazzjoni f'konformità mal-punt IS.D.OR.210;

(4) timplimenta skema ta' rapportar intern dwar is-sigurtà tal-informazzjoni f'konformità mal-punt IS.D.OR.215;

(5) tiddefinixxi u timplimenta, f'konformità mal-punt IS.D.OR.220, il-miżuri meħtieġa biex tidentifika avvenimenti relatati mas-sigurtà tal-informazzjoni, tidentifika dawk l-avvenimenti li jitqiesu inċidenti b'impatt potenzjali fuq is-sikurezza tal-avjazzjoni ħlief kif permess mill-punt IS.D.OR.205(e), u twieġeb għal, u tirkupra minn, dawk l-inċidenti tas-sigurtà tal-informazzjoni;

(6) timplimenta l-miżuri li jkunu ġew innotifikati mill-awtorità kompetenti bħala reazzjoni immedjata għal inċident jew vulnerabbiltà relatati mas-sigurtà tal-informazzjoni b'impatt fuq is-sikurezza tal-avjazzjoni;

(7) tieħu azzjoni xierqa, f'konformità mal-punt IS.D.OR.225, biex tindirizza s-sejbiet notifikati mill-awtorità kompetenti;

(8) timplimenta skema ta' rapportar estern f'konformità mal-punt IS.D.OR.230 sabiex tippermetti lill-awtorità kompetenti tieħu azzjonijiet xierqa;

(9) tikkonforma mar-rekwiżiti li jinsabu fil-punt IS.D.OR.235 meta tikkuntratta kwalunkwe parti mill-attivitajiet imsemmija fil-punt IS.D.OR.200 lil organizzazzjonijiet oħrajn;

(10) tikkonforma mar-rekwiżiti tal-persunal stabbiliti fil-punt IS.D.OR.240;

(11) tikkonforma mar-rekwiżiti taż-żamma tar-rekords stabbiliti fil-punt IS.D.OR.245;

(12) timmonitorja l-konformità tal-organizzazzjoni mar-rekwiżiti ta' dan ir-Regolament u tipprovdi feedback dwar is-sejbiet lill-maniġer responsabbli jew, fil-każ ta' organizzazzjonijiet tad-disinn, lill-kap tal-organizzazzjoni tad-disinn, sabiex tiżgura l-implimentazzjoni effettiva tal-azzjonijiet korrettivi;

(13) tipproteġi, mingħajr preġudizzju għar-rekwiżiti applikabbli ta' rapportar tal-inċidenti, il-kunfidenzjalità ta' kwalunkwe informazzjoni li l-organizzazzjoni setgħet irċeviet mingħand organizzazzjonijiet oħrajn, skont il-livell ta' sensittività tagħha.

(b) Sabiex tissodisfa kontinwament ir-rekwiżiti msemmija fl-Artikolu 1, l-organizzazzjoni għandha timplimenta proċess ta' titjib kontinwu f'konformità mal-punt IS.D.OR.260.

(c) L-organizzazzjoni għandha tiddokumenta, f'konformità mal-punt IS.D.OR.250, il-proċessi, il-proċeduri, ir-rwoli u r-responsabbiltajiet ewlenin kollha meħtieġa għall-konformità mal-punt IS.D.OR.200(a) u tistabbilixxi proċess għall-emendar ta' dik id-dokumentazzjoni. Il-bidliet f'dawk il-proċessi, il-proċeduri, ir-rwoli u r-responsabbiltajiet għandhom jiġu ġestiti f'konformità mal-punt IS.D.OR.255.

(d) Il-proċessi, il-proċeduri, ir-rwoli u r-responsabbiltajiet stabbiliti mill-organizzazzjoni

sabiex tikkonforma mal-punt IS.D.OR.200(a) għandhom jikkorrispondu man-natura u l-kumplessità tal-attivitajiet tagħha, abbażi ta' valutazzjoni tar-riskji għas-sigurtà tal-informazzjoni inerenti għal dawk l-attivitajiet, u jistgħu jiġu integrati fi ħdan sistemi ta' ġestjoni eżistenti oħrajn diġà implimentati mill-organizzazzjoni.

(e) Mingħajr preġudizzju għall-obbligu ta' konformità mar-rekwiżiti ta' rapportar li jinsabu fir-Regolament (UE) Nru 376/2014([1]) u r-rekwiżiti tal-punt IS.D.OR.200 (a) (13), l-organizzazzjoni tista' tingħata approvazzjoni mill-awtorità kompetenti biex ma timplimentax ir-rekwiżiti msemmija fil-punti (a) sa (d) u r-rekwiżiti relatati li jinsabu fil-punti IS.D.OR.205 sa IS.D.OR.260, jekk turi għas-sodisfazzjon ta' dik l-awtorità li l-attivitajiet, il-faċilitajiet u r-riżorsi tagħha, kif ukoll is-servizzi li topera, tipprovdi, tirċievi u żżomm, ma joħolqu l-ebda riskju għas-sigurtà tal-informazzjoni b'impatt potenzjali fuq is-sikurezza tal-avjazzjoni la għaliha nnifisha u lanqas għal organizzazzjonijiet oħrajn. L-approvazzjoni għandha tkun ibbażata fuq valutazzjoni tar-riskju għas-sigurtà tal-informazzjoni dokumentata mwettqa mill-organizzazzjoni jew minn parti terza f'konformità mal-punt IS.D.OR.205 u riveduta u approvata mill-awtorità kompetenti tagħha.

Il-validità kontinwa ta' dik l-approvazzjoni se tiġi riveduta mill-awtorità kompetenti wara ċ-ċiklu tal-awditjar tas-sorveljanza applikabbli u kull meta l-bidliet jiġu implimentati fil-kamp ta' applikazzjoni tal-ħidma tal-organizzazzjoni.

IS.D.OR.205 Valutazzjoni tar-riskju għas-sigurtà tal-informazzjoni

(a) L-organizzazzjoni għandha tidentifika l-elementi kollha tagħha, li jistgħu jkunu esposti għar-riskji għas-sigurtà tal-informazzjoni. Dan għandu jinkludi:

(1) l-attivitajiet, il-faċilitajiet u r-riżorsi tal-organizzazzjoni, kif ukoll is-servizzi li l-organizzazzjoni topera, tipprovdi, tirċievi jew iżżomm;

(2) it-tagħmir, is-sistemi, id-*data* u l-informazzjoni li jikkontribwixxu għall-funzjonament tal-elementi elenkati fil-punt (1).

(b) L-organizzazzjoni għandha tidentifika l-interfaċċi li għandha ma' organizzazzjonijiet oħrajn, u li jistgħu jirriżultaw fl-esponiment reċiproku għar-riskji għas-sigurtà tal-informazzjoni.

(c) Fir-rigward tal-elementi u l-interfaċċi msemmija fil-punti (a) u (b), l-organizzazzjoni għandha tidentifika r-riskji għas-sigurtà tal-informazzjoni li jista' jkollhom impatt potenzjali fuq is-sikurezza tal-avjazzjoni. Għal kull riskju identifikat, l-organizzazzjoni għandha:

(1) tassenja livell ta' riskju skont klassifikazzjoni predefinita stabbilita mill-organizzazzjoni;

([1]) Ir-Regolament (UE) Nru 376/2014 tal-Parlament Ewropew u tal-Kunsill tat-3 ta' April 2014 dwar ir-rappurtar, l-analiżi u s-segwitu ta' okkorrenzi fl-avjazzjoni ċivili, li jemenda r-Regolament (UE) Nru 996/2010 tal-Parlament Ewropew u tal-Kunsill u li jħassar id-Direttiva 2003/42/KE tal-Parlament Ewropew u tal-Kunsill, u r-Regolamenti tal-Kummissjoni (KE) Nru 1321/2007 u (KE) Nru 1330/2007 (ĠU L 122, 24.4.2014, p. 18).

(2) tassoċja kull riskju u l-livell tiegħu mal-element jew l-interfaċċa korrispondenti identifikati f'konformità mal-punti (a) u (b).

Il-klassifikazzjoni predefinita msemmija fil-punt (1) għandha tqis il-potenzjal tal-okkorrenza tax-xenarju ta' theddida u s-severità tal-konsegwenzi tas-sikurezza tiegħu. Abbażi ta' dik il-klassifikazzjoni, u b'kunsiderazzjoni ta' jekk l-organizzazzjoni għandhiex proċess ta' ġestjoni tar-riskju strutturat u ripetibbli għall-operazzjonijiet, l-organizzazzjoni għandha tkun tista' tistabbilixxi jekk ir-riskju huwiex aċċettabbli jew jeħtiġx li jiġi ttrattat f'konformità mal-punt IS.D.OR.210.

Sabiex tiġi ffaċilitata l-komparabbiltà reċiproka tal-valutazzjonijiet tar-riskji, l-assenjazzjoni tal-livell ta' riskju skont il-punt (1) għandha tqis l-informazzjoni rilevanti miksuba f'koordinazzjoni mal-organizzazzjonijiet imsemmija fil-punt (b).

(d) L-organizzazzjoni għandha tirrevedi u taġġorna l-valutazzjoni tar-riskju mwettqa f'konformità mal-punti (a), (b) u (c) fi kwalunkwe waħda mis-sitwazzjonijiet li ġejjin:

(1) ikun hemm bidla fl-elementi soġġetti għal riskji għas-sigurtà tal-informazzjoni;

(2) ikun hemm bidla fl-interfaċċi bejn l-organizzazzjoni u organizzazzjonijiet oħrajn, jew fir-riskji kkomunikati mill-organizzazzjonijiet l-oħra;

(3) ikun hemm bidla fl-informazzjoni jew fl-għarfien użati għall-identifikazzjoni, l-analiżi u l-klassifikazzjoni tar-riskji;

(4) ikun hemm tagħlimiet meħuda mill-analiżi tal-inċidenti tas-sigurtà tal-informazzjoni.

IS.D.OR.210 Trattament tar-riskju għas-sigurtà tal-informazzjoni

(a) L-organizzazzjoni għandha tiżviluppa miżuri biex tindirizza r-riskji inaċċettabbli identifikati f'konformità mal-punt IS.D.OR.205, timplimentahom fil-ħin u tivverifika l-effettività kontinwa tagħhom. Dawk il-miżuri għandhom jippermettu lill-organizzazzjoni:

(1) tikkontrolla ċ-ċirkostanzi li jikkontribwixxu għall-okkorrenza effettiva tax-xenarju ta' theddida;

(2) tnaqqas il-konsegwenzi fuq is-sikurezza tal-avjazzjoni assoċjati mal-materjalizzazzjoni tax-xenarju ta' theddida;

(3) tevita r-riskji.

Dawk il-miżuri ma għandhom jintroduċu l-ebda riskju inaċċettabbli potenzjali ġdid għas-sikurezza tal-avjazzjoni.

(b) Il-persuna msemmija fil-punt IS.D.OR.240(a) u (b) u persunal affettwat ieħor tal-organizzazzjoni għandhom jiġu informati bl-eżitu tal-valutazzjoni tar-riskju mwettqa f'konformità mal-punt IS.D.OR.205, ix-xenarji ta' theddid korrispondenti u l-miżuri li għandhom jiġu implimentati.

L-organizzazzjoni għandha tinforma wkoll lill-organizzazzjonijiet li magħhom ikollha interfaċċa f'konformità mal-punt IS.D.OR.205(b) bi kwalunkwe riskju kondiviż bejn iż-żewġ organizzazzjonijiet.

IS.D.OR.215 Skema ta' rapportar intern dwar is-sigurtà tal-informazzjoni

(a) L-organizzazzjoni għandha tistabbilixxi skema ta' rapportar intern li tippermetti l-ġbir u l-evalwazzjoni ta' avvenimenti relatati mas-sigurtà tal-informazzjoni, inklużi dawk li għandhom jiġu rrapportati skont il-punt IS.D.OR.230.

(b) Dik l-iskema u l-proċess imsemmi fil-punt IS.D.OR.220 għandhom jippermettu lill-organizzazzjoni:

(1) tidentifika liema mill-avvenimenti rrapportati skont il-punt (a) jitqiesu bħala inċidenti jew vulnerabbiltajiet tas-sigurtà tal-informazzjoni b'impatt potenzjali fuq is-sikurezza tal-avjazzjoni;

(2) tidentifika l-kawżi tal-inċidenti u l-vulnerabbiltajiet tas-sigurtà tal-informazzjoni identifikati f'konformità mal-punt (1), u tindirizzahom bħala parti mill-proċess ta' ġestjoni tar-riskju għas-sigurtà tal-informazzjoni f'konformità mal-punti IS.D.OR.205 u IS.D.OR.220;

(3) tiżgura evalwazzjoni tal-inċidenti u l-vulnerabbiltajiet kollha magħrufa u rilevanti relatati mas-sigurtà tal-informazzjoni identifikati f'konformità mal-punt (1);

(4) tiżgura l-implimentazzjoni ta' metodu għad-distribuzzjoni interna tal-informazzjoni kif meħtieġ.

(c) Kwalunkwe organizzazzjoni kuntrattata li tista' tesponi lill-organizzazzjoni għal riskji għas-sigurtà tal-informazzjoni b'impatt potenzjali fuq is-sikurezza tal-avjazzjoni għandha tkun meħtieġa tirrapporta avvenimenti relatati mas-sigurtà tal-informazzjoni lill-organizzazzjoni. Dawk ir-rapporti għandhom jiġu ppreżentati bl-użu tal-proċeduri stabbiliti fl-arranġamenti kuntrattwali speċifiċi u għandhom jiġu evalwati f'konformità mal-punt (b).

(d) L-organizzazzjoni għandha tikkoopera fl-investigazzjonijiet ma' kwalunkwe organizzazzjoni oħra li jkollha kontribut sinifikanti għas-sigurtà tal-informazzjoni tal-attivitajiet tagħha stess.

(e) L-organizzazzjoni tista' tintegra dik l-iskema ta' rapportar ma' skemi oħra ta' rapportar li tkun diġà implimentat.

IS.D.OR.220 Inċidenti ta' sigurtà tal-informazzjoni — detezzjoni, rispons, u rkupru

(a) Abbażi tal-eżitu tal-valutazzjoni tar-riskju mwettqa f'konformità mal-punt IS.D.OR.205 u l-eżitu tat-trattament tar-riskju mwettaq f'konformità mal-punt IS.D.OR.210, l-organizzazzjoni għandha timplimenta miżuri biex jiġu identifikati inċidenti u vulnerabbiltajiet li jindikaw il-materjalizzazzjoni potenzjali ta' riskji inaċċettabbli u li

jista' jkollhom impatt potenzjali fuq is-sikurezza tal-avjazzjoni. Dawk il-miżuri ta' detezzjoni għandhom jippermettu lill-organizzazzjoni:

(1) tidentifika devjazzjonijiet mil-linji bażi predeterminati tal-prestazzjoni funzjonali;

(2) tiskatta twissijiet biex jiġu attivati miżuri ta' rispons xierqa, f'każ ta' kwalunkwe devjazzjoni.

(b) L-organizzazzjoni għandha timplimenta miżuri biex tirrispondi għal kwalunkwe kundizzjoni ta' avveniment identifikata f'konformità mal-punt (a) li tista' tiżviluppa jew tkun żviluppat f'inċident tas-sigurtà tal-informazzjoni. Dawk il-miżuri ta' rispons għandhom jippermettu lill-organizzazzjoni:

(1) tibda r-reazzjoni għat-twissijiet imsemmija fil-punt (a)(2) billi tattiva riżorsi predefiniti u kors ta' azzjonijiet;

(2) tikkontrolla t-tixrid ta' attakk u tevita l-materjalizzazzjoni sħiħa ta' xenarju ta' theddida;

(3) tikkontrolla l-modalità ta' ħsara tal-elementi affettwati ddefiniti fil-punt IS.D.OR.205(a).

(c) L-organizzazzjoni għandha timplimenta miżuri mmirati lejn l-irkupru minn inċidenti ta' sigurtà tal-informazzjoni, inklużi miżuri ta' emerġenza, jekk ikun meħtieġ. Dawk il-miżuri ta' rkupru għandhom jippermettu lill-organizzazzjoni:

(1) tneħħi l-kundizzjoni li kkawżat l-inċident, jew tillimitaha għal livell tollerabbli;

(2) tilħaq stat sikur tal-elementi affettwati ddefiniti fil-punt IS.D.OR.205(a) fi żmien ta' rkupru definit qabel mill-organizzazzjoni.

IS.D.OR.225 Risposta għas-sejbiet innotifikati mill-awtorità kompetenti

(a) Wara li tirċievi n-notifika tas-sejbiet sottomessi mill-awtorità kompetenti, l-organizzazzjoni għandha:

(1) tidentifika l-kawża jew il-kawżi fundamentali tan-nonkonformità, u l-fatturi li jikkontribwixxu għaliha;

(2) tfassal pjan ta' azzjoni korrettiva;

(3) turi l-korrezzjoni tan-nonkonformità għas-sodisfazzjon tal-awtorità kompetenti.

(b) L-azzjonijiet imsemmija fil-punt (a) għandhom jitwettqu fil-perjodu miftiehem mal-awtorità kompetenti.

IS.D.OR.230 Skema ta' rapportar estern dwar is-sigurtà tal-informazzjoni

(a) L-organizzazzjoni għandha timplimenta sistema ta' rapportar tas-sigurtà tal-informazzjoni li tikkonforma mar-rekwiżiti stabbiliti fir-Regolament (UE) Nru 376/2014

u l-atti delegati u ta' implimentazzjoni tiegħu jekk dak ir-Regolament ikun applikabbli għall-organizzazzjoni.

(b) Mingħajr preġudizzju għall-obbligi tar-Regolament (UE) 376/2014, l-organizzazzjoni għandha tiżgura li kwalunkwe inċident jew vulnerabbiltà għas-sigurtà tal-informazzjoni, li jistgħu jirrappreżentaw riskju sinifikanti għas-sikurezza tal-avjazzjoni, jiġu rrapportati lill-awtorità kompetenti tagħhom. Barra minn hekk:

(1) meta tali inċident jew vulnerabbiltà taffettwa inġenju tal-ajru jew sistema jew komponent assoċjat, l-organizzazzjoni għandha tirrapportaha wkoll lid-detentur tal-approvazzjoni tad-disinn;

(2) meta tali inċident jew vulnerabbiltà taffettwa sistema jew kostitwent użat mill-organizzazzjoni, l-organizzazzjoni għandha tirrapportaha lill-organizzazzjoni responsabbli għad-disinn tas-sistema jew tal-kostitwent.

(c) L-organizzazzjoni għandha tirrapporta l-kundizzjonijiet imsemmija fil-punt (b) kif ġej:

(1) notifika għandha tiġi sottomessa lill-awtorità kompetenti u, jekk applikabbli, lid-detentur tal-approvazzjoni tad-disinn jew lill-organizzazzjoni responsabbli għad-disinn tas-sistema jew tal-kostitwent, malli l-kundizzjoni ssir magħrufa mill-organizzazzjoni;

(2) rapport għandu jiġi ppreżentat lill-awtorità kompetenti u, jekk applikabbli, lid-detentur tal-approvazzjoni tad-disinn jew lill-organizzazzjoni responsabbli għad-disinn tas-sistema jew tal-kostitwent, mill-aktar fis possibbli, iżda mhux aktar minn 72 siegħa minn meta l-kundizzjoni ssir magħrufa mill-organizzazzjoni, sakemm ċirkostanzi eċċezzjonali ma jipprevjenux dan.

Ir-rapport għandu jsir fil-forma ddefinita mill-awtorità kompetenti u għandu jkun fih l-informazzjoni rilevanti kollha dwar il-kundizzjoni magħrufa mill-organizzazzjoni;

(3) għandu jiġi ppreżentat rapport ta' segwitu lill-awtorità kompetenti u, jekk applikabbli, lid-detentur tal-approvazzjoni tad-disinn jew lill-organizzazzjoni responsabbli għad-disinn tas-sistema jew tal-kostitwent, li jipprovdi dettalji tal-azzjonijiet li l-organizzazzjoni tkun ħadet jew li tkun beħsiebha tieħu biex tirkupra mill-inċident u l-azzjonijiet li biħsiebha tieħu biex tipprevjeni inċidenti simili tas-sigurtà tal-informazzjoni fil-futur.

Ir-rapport ta' segwitu għandu jiġi ppreżentat hekk kif dawk l-azzjonijiet ikunu ġew identifikati, u għandu jiġi prodott fil-forma ddefinita mill-awtorità kompetenti.

IS.D.OR.235 Kuntrattar ta' attivitajiet ta' ġestjoni tas-sigurtà tal-informazzjoni

(a) L-organizzazzjoni għandha tiżgura li meta tikkuntratta kwalunkwe parti mill-attivitajiet imsemmija fil-punt IS.D.OR.200 lil organizzazzjonijiet oħrajn, l-attivitajiet kuntrattati jikkonformaw mar-rekwiżiti ta' dan ir-Regolament u l-organizzazzjoni kuntrattata

taħdem taħt is-sorveljanza tagħha. L-organizzazzjoni għandha tiżgura li r-riskji assoċjati mal-attivitajiet ikkuntrattati jiġu ġestiti b'mod xieraq.

(b) L-organizzazzjoni għandha tiżgura li l-awtorità kompetenti jista' jkollha aċċess fuq talba lill-organizzazzjoni kuntrattata biex tiddetermina l-konformità kontinwa mar-rekwiżiti applikabbli stabbiliti f'dan ir-Regolament.

IS.D.OR.240 Rekwiżiti tal-persunal

(a) Il-maniġer responsabbli tal-organizzazzjoni jew, fil-każ ta' organizzazzjonijiet tad-disinn, il-kap tal-organizzazzjoni tad-disinn, maħtur f'konformità mar-Regolament (UE) Nru 748/2012 u r-Regolament (UE) Nru 139/2014 kif imsemmi fil-punti 1(a) u (b) tal-Artikolu 2 ta' dan ir-Regolament, għandu jkollu awtorità korporattiva biex jiżgura li l-attivitajiet kollha meħtieġa minn dan ir-Regolament ikunu jistgħu jiġu ffinanzjati u mwettqa. Dik il-persuna għandha:

(1) tiżgura li r-riżorsi kollha meħtieġa jkunu disponibbli biex jikkonformaw mar-rekwiżiti ta' dan ir-Regolament;

(2) tistabbilixxi u tippromwovi l-politika dwar is-sigurtà tal-informazzjoni msemmija fil-punt IS.D.OR.200(a)(1);

(3) juri fehim bażiku ta' dan ir-Regolament.

(b) Il-maniġer responsabbli jew, fil-każ ta' organizzazzjonijiet tad-disinn, il-kap tal-organizzazzjoni tad-disinn, għandu jaħtar persuna jew grupp ta' persuni biex jiżgura li l-organizzazzjoni tkun konformi mar-rekwiżiti ta' dan ir-Regolament, u għandu jiddefinixxi l-estent tal-awtorità tagħhom. Dik il-persuna jew grupp ta' persuni għandhom jirrapportaw direttament lill-maniġer responsabbli jew, fil-każ ta' organizzazzjonijiet tad-disinn, lill-kap tal-organizzazzjoni tad-disinn, u għandu jkollhom l-għarfien, il-kompetenzi u l-esperjenza xierqa biex iwettqu r-responsabbiltajiet tagħhom. Għandu jiġi ddeterminat fil-proċeduri min jidher f'isem persuna partikolari fil-każ ta' assenza twila ta' dik il-persuna.

(c) Il-maniġer responsabbli jew, fil-każ ta' organizzazzjonijiet tad-disinn, il-kap tal-organizzazzjoni tad-disinn għandu jaħtar persuna jew grupp ta' persuni bir-responsabbiltà li jimmaniġġjaw il-funzjoni ta' monitoraġġ tal-konformità msemmija fil-punt IS.D.OR.200(a)(12).

(d) Meta l-organizzazzjoni taqsam strutturi organizzattivi, politiki, proċessi u proċeduri tas-sigurtà tal-informazzjoni, ma' organizzazzjonijiet oħrajn jew ma' oqsma tal-organizzazzjoni tagħha stess li ma humiex parti mill-approvazzjoni jew mid-dikjarazzjoni, il-maniġer responsabbli jew, fil-każ ta' organizzazzjonijiet tad-disinn, il-kap tal-organizzazzjoni tad-disinn, jista' jiddelega l-attivitajiet tagħha lil persuna responsabbli komuni.

F'każ bħal dan, għandhom jiġu stabbiliti miżuri ta' koordinazzjoni bejn il-maniġer responsabbli tal-organizzazzjoni jew, fil-każ ta' organizzazzjonijiet tad-disinn, il-kap tal-organizzazzjoni tad-disinn, u l-persuna responsabbli komuni biex tiġi żgurata

integrazzjoni adegwata tal-ġestjoni tas-sigurtà tal-informazzjoni fi ħdan l-organizzazzjoni.

(e) Il-maniġer responsabbli jew il-kap tal-organizzazzjoni, tad-disinn, jew il-persuna responsabbli komuni msemmija fil-punt (d), għandu jkollhom awtorità korporattiva biex jistabbilixxu u jżommu l-istrutturi organizzattivi, il-politiki, il-proċessi u l-proċeduri meħtieġa għall-implimentazzjoni tal-punt IS.D.OR.200.

(f) L-organizzazzjoni għandu jkollha proċess fis-seħħ biex tiżgura li jkollha biżżejjed persunal fid-dmir li twettaq l-attivitajiet koperti minn dan l-Anness.

(g) L-organizzazzjoni għandu jkollha proċess fis-seħħ biex tiżgura li l-persunal imsemmi fil-punt (f) ikollu l-kompetenza meħtieġa biex iwettaq il-kompiti tiegħu.

(h) L-organizzazzjoni għandu jkollha proċess fis-seħħ biex tiżgura li l-persunal jirrikonoxxi r-responsabbiltajiet assoċjati mar-rwoli u mal-kompiti assenjati.

(i) L-organizzazzjoni għandha tiżgura li l-identità u l-affidabbiltà tal-persunal li għandu aċċess għas-sistemi tal-informazzjoni u għad-*data* soġġetti għar-rekwiżiti ta' dan ir-Regolament ikunu stabbiliti b'mod xieraq.

IS.D.OR.245 Żamma ta' rekords

(a) L-organizzazzjoni għandha żżomm rekords tal-attivitajiet ta' ġestjoni tas-sigurtà tal-informazzjoni

(1) L-organizzazzjoni għandha tiżgura li r-rekords li ġejjin ikunu arkivjati u traċċabbli:

(i) kwalunkwe approvazzjoni riċevuta u kwalunkwe valutazzjoni assoċjata tar-riskju għas-sigurtà tal-informazzjoni f'konformità mal-punt IS.D.OR.200(e);

(ii) kuntratti għall-attivitajiet imsemmija fil-punt IS.D.OR.200(a)(9);

(iii) rekords tal-proċessi ewlenin imsemmija fil-punt IS.D.OR.200(d);

(iv) rekords tar-riskji identifikati fil-valutazzjoni tar-riskju msemmija fil-punt IS.D.OR.205 flimkien mal-miżuri assoċjati tat-trattament tar-riskju msemmija fil-punt IS.D.OR.210;

(v) rekords ta' inċidenti u vulnerabbiltajiet tas-sigurtà tal-informazzjoni rrapportati f'konformità mal-iskemi ta' rapportar imsemmija fil-punti IS.D.OR.215 u IS.D.OR.230;

(vi) rekords ta' dawk l-avvenimenti relatati mas-sigurtà tal-informazzjoni li jista' jkollhom bżonn jiġu vvalutati mill-ġdid biex jiżvelaw inċidenti jew vulnerabbiltajiet ta' sigurtà tal-informazzjoni mhux identifikati.

(2) Ir-rekords imsemmija fil-punt (1)(i) għandhom jinżammu mill-inqas sa 5 snin wara li l-approvazzjoni tkun tilfet il-validità tagħha.

(3) Ir-rekords imsemmija fil-punt (1)(ii) għandhom jinżammu mill-inqas sa 5 snin wara li l-kuntratt ikun ġie emendat jew itterminat.

(4) Ir-rekords imsemmija fil-punt (1)(iii), (iv) u (v) għandhom jinżammu mill-inqas għal perjodu ta' 5 snin.

(5) Ir-rekords imsemmija fil-punt (1)(vi) għandhom jinżammu sakemm dawk l-avvenimenti relatati mas-sigurtà tal-informazzjoni jkunu ġew ivvalutati mill-ġdid f'konformità mal-perjodiċità definita fi proċedura stabbilita mill-organizzazzjoni.

(b) L-organizzazzjoni għandha żżomm rekords tal-kwalifiki u tal-esperjenza tal-persunal tagħha stess involut fl-attivitajiet ta' ġestjoni tas-sigurtà tal-informazzjoni

(1) Ir-rekords tal-kwalifiki u tal-esperjenza tal-persunal jinżammu sakemm il-persuna taħdem għall-organizzazzjoni, u għal mill-inqas tliet snin wara li l-persuna tkun telqet mill-organizzazzjoni.

(2) Il-membri tal-persunal għandhom, fuq talba tagħhom, jingħataw aċċess għar-rekords individwali tagħhom. Barra minn hekk, fuq talba tagħhom, l-organizzazzjoni għandha tfornihom b'kopja tar-rekords individwali tagħhom malli jitilqu mill-organizzazzjoni.

(c) Il-format tar-rekords għandu jiġi speċifikat fil-proċeduri tal-organizzazzjoni.

(d) Ir-rekords għandhom jinħażnu b'mod li jiżgura l-protezzjoni mill-ħsara, mit-tibdil u mis-serq, bl-informazzjoni tiġi identifikata, meta meħtieġ, skont il-livell tal-klassifikazzjoni tas-sigurtà tagħha. L-organizzazzjoni għandha tiżgura li r-rekords jinħażnu bl-użu ta' mezzi biex jiġu żgurati l-integrità, l-awtentiċità u l-aċċess awtorizzat.

IS.D.OR.250 Manwal għall-ġestjoni tas-sigurtà tal-informazzjoni (ISMM)

(a) L-organizzazzjoni għandha tqiegħed għad-dispożizzjoni tal-awtorità kompetenti manwal għall-ġestjoni tas-sigurtà tal-informazzjoni (ISMM) u, fejn applikabbli, kwalunkwe manwal u proċedura assoċjati referenzjati, li jkun fih:

(1) dikjarazzjoni ffirmata mill-maniġer responsabbli jew, fil-każ ta' organizzazzjonijiet tad-disinn, mill-kap tal-organizzazzjoni tad-disinn, li tikkonferma li l-organizzazzjoni se taħdem f'kull ħin f'konformità ma' dan l-Anness u mal-ISMM. Jekk il-maniġer responsabbli jew, fil-każ ta' organizzazzjonijiet tad-disinn, il-kap tal-organizzazzjoni tad-disinn, ma jkunx l-uffiċjal eżekuttiv ewlieni (CEO) tal-organizzazzjoni, dan is-CEO għandu jikkontrofirma d-dikjarazzjoni;

(2) it-titolu/i, l-isem/ismijiet, id-dmirijiet, l-obbligi ta' rendikont, ir-responsabbiltajiet u l-awtoritajiet tal-persuna jew tal-persuni msemmija fil-punt IS.D.OR.240(b) u (c);

(3) it-titolu, l-isem, id-dmirijiet, l-obbligi ta' rendikont, ir-responsabbiltajiet u l-awtoritajiet tal-persuna responsabbli komuni msemmija fil-punt IS.D.OR.240(d), jekk applikabbli;

(4) il-politika dwar is-sigurtà tal-informazzjoni tal-organizzazzjoni kif imsemmija fil-punt IS.D.OR.200(a)(1);

(5) deskrizzjoni ġenerali tan-numru u tal-kategorija tal-persunal u tas-sistema fis-seħħ biex tippjana d-disponibbiltà tal-persunal, kif meħtieġ mill-punt IS.D.OR.240;

(6) it-titolu/i, l-isem/ismijiet, id-dmirijiet, l-obbligi ta' rendikont, ir-responsabbiltajiet u l-awtoritajiet tal-persuni ewlenin responsabbli għall-implimentazzjoni tal-punt IS.D.OR.200, inkluża l-persuna jew il-persuni responsabbli għall-funzjoni ta' monitoraġġ tal-konformità msemmija fil-punt IS.D.OR.200(a)(12);

(7) organigramma li turi l-katini assoċjati ta' obbligi ta' rendikont u responsabbiltà għall-persuni msemmija fil-punti (2) u (6);

(8) id-deskrizzjoni tal-iskema ta' rapportar intern imsemmija fil-punt IS.D.OR.215;

(9) il-proċeduri li jispeċifikaw kif l-organizzazzjoni tiżgura l-konformità ma' din il-Parti, u b'mod partikolari:

(i) il-punt tad-dokumentazzjoni IS.D.OR.200(c);

(ii) il-proċeduri li jiddefinixxu kif l-organizzazzjoni tikkontrolla kwalunkwe attività kuntrattata msemmija fil-punt IS.D.OR.200(a)(9);

(iii) il-proċedura ta' emenda tal-ISMM definita fil-punt (c);

(10) il-lista ta' mezzi alternattivi ta' konformità approvati bħalissa.

(b) Il-ħruġ inizjali tal-ISMM għandu jiġi approvat u għandha tinżamm kopja mill-awtorità kompetenti. L-ISMM għandha tiġi emendata kif meħtieġ biex tibqa' deskrizzjoni aġġornata tal-organizzazzjoni. Kopja ta' kwalunkwe emenda għall-ISMM għandha tiġu pprovduta lill-awtorità kompetenti.

(c) L-emendi għall-ISMM għandhom jiġu ġestiti fi proċedura stabbilita mill-organizzazzjoni. Kwalunkwe emenda li ma tkunx inkluża fil-kamp ta' applikazzjoni tal-proċedura u kwalunkwe emenda relatata mal-bidliet msemmija fil-punt IS.D.OR.255(b), għandhom jiġu approvati mill-awtorità kompetenti.

(d) L-organizzazzjoni tista' tintegra l-ISMM ma' espożizzjonijiet maniġerjali jew manwali oħra li jkollha, sakemm ikun hemm kontroreferenza ċara li tindika liema porzjonijiet mill-preżentazzjoni jew mill-manwal tal-ġestjoni jikkorrispondu għar-rekwiżiti differenti li jinsabu f'dan l-Anness.

IS.D.OR.255 Bidliet fis-sistema ta' ġestjoni tas-sigurtà tal-informazzjoni

(a) Il-bidliet fl-ISMS jistgħu jiġu ġestiti u nnotifikati lill-awtorità kompetenti fi proċedura żviluppata mill-organizzazzjoni. Din il-proċedura għandha tiġi approvata mill-awtorità kompetenti.

(b) Fir-rigward tal-bidliet fl-ISMS li ma humiex koperti mill-proċedura msemmija fil-punt (a), l-organizzazzjoni għandha tapplika għal u tikseb approvazzjoni maħruġa mill-awtorità kompetenti.

Fir-rigward ta' dawn il-bidliet:

(1) l-applikazzjoni għandha titressaq qabel ma ssir il-bidla, sabiex l-awtorità kompetenti tkun tista' tiddetermina l-konformità kontinwa ma' dan ir-Regolament, u sabiex temenda, jekk ikun meħtieġ, iċ-ċertifikat tal-organizzazzjoni tat-taħriġ u t-termini tal-approvazzjoni relatati mehmuża miegħu;

(2) l-organizzazzjoni għandha tqiegħed għad-dispożizzjoni tal-awtorità kompetenti kwalunkwe informazzjoni li titlob biex tevalwa l-bidla;

(3) it-tibdil għandu jiġi implimentat biss mal-wasla ta' approvazzjoni formali mill-awtorità kompetenti;

(4) l-organizzazzjoni għandha topera taħt il-kundizzjonijiet preskritti mill-awtorità kompetenti matul l-implimentazzjoni ta' dawn il-bidliet.

IS.D.OR.260 Titjib kontinwu

(a) L-organizzazzjoni għandha tivvaluta, bl-użu ta' indikaturi ta' prestazzjoni adegwati, l-effettività u l-maturità tal-ISMS. Dik il-valutazzjoni għandha titwettaq fuq bażi kalendarja predefinita mill-organizzazzjoni jew wara inċident tas-sigurtà tal-informazzjoni.

(b) Jekk jinstabu nuqqasijiet wara l-valutazzjoni mwettqa f'konformità mal-punt (a), l-organizzazzjoni għandha tieħu l-miżuri ta' titjib meħtieġa biex tiżgura li l-ISMS tkompli tikkonforma mar-rekwiżiti applikabbli u żżomm ir-riskji għas-sigurtà tal-informazzjoni f'livell aċċettabbli. Barra minn hekk, l-organizzazzjoni għandha tivvaluta mill-ġdid dawk l-elementi tal-ISMS affettwati mill-miżuri adottati.