Linji gwida 01/2021

dwar Eżempji li jikkonċernaw Notifika ta' Ksur ta' *Data* Personali

Adottati fl-14 ta' Diċembru 2021

Verżjoni 2.0

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Rekord tal-verżjonijiet

Verżjoni 2.0	14 12 2021	Adozzjoni tal-Linji Gwida wara konsultazzjoni pubblika
Verżjoni 1.0	14 01 2021	Adozzjoni tal-Linji Gwida għal konsultazzjoni pubblika

Werrej

IL-BORD EWROPEW GĦALL-PROTEZZJONI TAD-*DATA*

Wara li kkunsidra l-Artikolu 70(1e) tar-Regolament 2016/679/UE tal-Parlament Ewropew u tal-Kunsill tas-27 ta' April 2016 dwar il-protezzjoni tal-persuni fiżiċi fir-rigward tal-ipproċessar ta' *data* personali u dwar il-moviment liberu ta' tali *data*, u li jħassar id-Direttiva 95/46/KE (minn hawn 'il quddiem "GDPR"),

Wara li kkunsidra l-Ftehim ŻEE u b'mod partikolari l-Anness XI u l-Protokoll 37 tiegħu, kif emendati bid-Deċiżjoni tal-Kumitat Konġunt taż-ŻEE Nru 154/2018 tas-6 ta' Lulju 2018[1],

Wara li kkunsidra l-Artikolu 12 u l-Artikolu 22 tar-Regoli ta' Proċedura tiegħu,

Wara li kkunsidra l-Komunikazzjoni tal-Kummissjoni lill-Parlament Ewropew u lill-Kunsill bit-titolu Il-protezzjoni tad-*data* bħala pilastru tal-għoti tas-setgħa liċ-ċittadini u tal-approċċ tal-UE għat-tranżizzjoni diġitali - sentejn ta' applikazzjoni tar-Regolament Ġenerali dwar il-Protezzjoni tad-*Data*[2],

ADOTTA L-LINJI GWIDA LI ĠEJJIN

1 INTRODUZZJONI

1. Il-GDPR jintroduċi, f'ċerti każijiet, ir-rekwiżit li ksur ta' *data* personali jiġi nnotifikat lill-awtorità superviżorja nazzjonali kompetenti (minn hawn 'il quddiem "SA") u li l-ksur jiġi kkomunikat lill-individwi li d-*data* personali tagħhom tkun ġiet affettwata mill-ksur (l-Artikoli 33 u 34).

2. Il-Grupp ta' Ħidma tal-Artikolu 29 diġà pproduċa gwida *ġenerali* dwar in-notifika ta' ksur ta' *data* f'Ottubru tal-2017, li tanalizza t-Taqsimiet rilevanti tal-GDPR (il-Linji Gwida dwar in-notifika ta' ksur ta' *data* Personali skont ir-Regolament 2016/679, WP 250) (minn hawn 'il quddiem "Linji Gwida WP250")[3]. Madankollu, minħabba n-natura u ż-żmien tagħha, din il-linja gwida ma indirizzatx il-kwistjonijiet pratiċi kollha f'dettall suffiċjenti. Għalhekk, inħolqot il-ħtieġa ta' gwida *orjentata lejn il-prattika u bbażata fuq il-każ*, li tuża l-esperjenzi miksuba mill-SAs minn meta jsir applikabbli l-GDPR.

3. Dan id-dokument huwa maħsub sabiex jikkomplementa l-Linji Gwida WP 250 u jirrifletti l-esperjenzi komuni tal-SAs taż-ŻEE minn meta sar applikabbli l-GDPR. L-għan tiegħu huwa li jgħin lill-kontrolluri tad-*data* jiddeċiedu kif jimmaniġġaw il-ksur tad-*data* u liema fatturi għandhom jikkunsidraw matul il-valutazzjoni tar-riskju.

[1] Referenzi għal "Stati Membri" li jsiru f'dan id-dokument għandhom jinftiehmu bħala referenzi għall-"Istati Membri taż-ŻEE".

[2] COM(2020) 264 final, l-24 ta' Ġunju 2020.

[3] G29 WP250 rev.1, is-6 ta' Frar 2018, il-Linji Gwida dwar in-Notifika ta' Ksur ta' *Data* Personali skont ir-Regolament 2016/679 — approvati mill-EDPB, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

4. Bħala parti minn kwalunkwe tentattiv sabiex jiġi indirizzat ksur, il-kontrollur u l-proċessur għandhom l-ewwel nett ikollhom il-kapaċità jirrikonoxxu l-ksur. Il-GDPR jiddefinixxi "ksur ta' *data* personali" fl-Artikolu 4(12) bħala "ksur tas-sigurtà li jwassal għal qerda aċċidentali jew illegali, telf, bidliet, żvelar mhux awtorizzat ta', jew aċċess għal, *data* personali trażmessa, maħżuna jew ipproċessata b'xi mod ieħor".

5. Fl-Opinjoni 03/2014 tiegħu dwar in-notifika ta' ksur[4] u fil-Linji Gwida WP 250 tiegħu, id-WP29 spjega li l-ksur jista' jiġi kkategorizzat skont it-tliet prinċipji magħrufa sew tas-sigurtà tal-informazzjoni li ġejjin:

   - "Ksur tal-kunfidenzjalità" - fejn ikun hemm żvelar mhux awtorizzat jew aċċidentali ta' *data* personali, jew aċċess mhux awtorizzat għaliha.
   - "Ksur ta' integrità" - fejn ikun hemm alterazzjoni mhux awtorizzata jew aċċidentali ta' *data* personali.
   - "Ksur tad-disponibbiltà" - fejn ikun hemm telf aċċidentali jew mhux awtorizzat ta' aċċess għal *data* personali, jew il-qerda aċċidentali jew mhux awtorizzata tagħha.[5]

6. Ksur għandu l-potenzjal li jkollu firxa ta' effetti avversi sinifikanti fuq l-individwi, li jistgħu jirriżultaw fi ħsara fiżika, materjali jew mhux materjali. Il-GDPR jispjega li dan jista' jinkludi telf ta' kontroll fuq id-*data* personali tagħhom, limitazzjoni tad-drittijiet tagħhom, diskriminazzjoni, serq jew frodi tal-identità, telf finanzjarju, treġġigħ lura mhux awtorizzat tal-psewdonimizzazzjoni, ħsara għar-reputazzjoni, u telf tal-kunfidenzjalità tad-*data* personali protetta b'segretezza professjonali. Jista' jinkludi wkoll kwalunkwe żvantaġġ ekonomiku jew soċjali sinifikanti ieħor għal dawk l-individwi. Wieħed mill-aktar obbligi importanti tal-kontrollur tad-*data* huwa li jevalwa dawn ir-riskji għad-drittijiet u l-libertajiet tas-suġġetti tad-*data* u li jimplimenta miżuri tekniċi u organizzazzjonali xierqa sabiex jindirizzahom.

7. Għaldaqstant, il-GDPR jirrikjedi li l-kontrollur:

   - jiddokumenta kwalunkwe ksur ta' *data* personali, inklużi l-fatti relatati mal-ksur tad-*data* personali, l-effetti tiegħu u l-azzjoni ta' rimedju meħuda[6];
   - jinnotifika l-ksur tad-*data* personali lill-awtorità superviżorja, ħlief jekk il-ksur ta' *data* personali x'aktarx ma jirriżultax f'riskju għad-drittijiet u l-libertajiet tal-persuni fiżiċi[7];
   - jikkomunika l-ksur ta' *data* personali lis-suġġett tad-*data* meta l-ksur tad-*data* personali probabbilment ikun se jirriżulta f'riskju għoli għad-drittijiet u l-libertajiet tal-persuni fiżiċi[8].

8. Il-ksur tad-*data* huwa problema fih innifsu u minnu nnifsu, iżda jista' jkun ukoll sintomu ta' sistema tas-sigurtà tad-*data* vulnerabbli u possibbilment antikwata, dan jista' jindika wkoll dgħufijiet fis-sistema li għandhom jiġu indirizzati. Bħala verità ġenerali, dejjem ikun aħjar li jiġi pprevenut il-ksur tad-*data* billi jsir preparament minn qabel, peress li diversi konsegwenzi tiegħu huma min-natura tagħhom irriversibbli. Qabel ma kontrollur ikun jista' jivvaluta *bis-sħiħ* ir-riskju li jinħoloq minn ksur ikkawżat minn xi forma ta'

---

[4] G29 WP213, il-25 ta' Marzu 2014, l-Opinjoni 03/2014 dwar in-Notifika ta' Ksur ta' Dejta Personali, p. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_mt.pdf.

[5] Ara l-Linji Gwida WP 250, p. 7. - Irid jitqies li ksur tad-*data* jista' jikkonċerna kategorija waħda jew aktar simultanjament jew flimkien.

[6] L-Artikolu 33(5) tal-GDPR.

[7] L-Artikolu 33(1) tal-GDPR.

[8] L-Artikolu 34(1) tal-GDPR.

attakk, għandha tiġi identifikata l-kawża ewlenija tal-kwistjoni, sabiex jiġi identifikat jekk xi vulnerabbiltajiet li wasslu għall-inċident għadhomx preżenti, u għalhekk għadhom jistgħu jiġu sfruttati. F'ħafna każijiet, il-kontrollur ikun jista' jidentifika li l-inċident x'aktarx jirriżulta f'riskju, u għalhekk għandu jiġi nnotifikat. F'każijiet oħrajn, in-notifika ma teħtieġx li tiġi posposta sakemm ir-riskju u l-impatt li jikkonċernaw il-ksur ikunu ġew ivvalutati bis-sħiħ, peress li l-valutazzjoni tar-riskju sħiħa tista' sseħħ b'mod parallel man-notifika, u l-informazzjoni miksuba b'dan il-mod tista' tiġi pprovduta lill-SA f'fażijiet mingħajr aktar dewmien żejjed[9].

9. Il-ksur għandu jiġi nnotifikat meta l-kontrollur ikun tal-fehma li x'aktarx jirriżulta f'riskju għad-drittijiet u l-libertajiet tas-suġġett tad-*data*. Il-kontrolluri għandhom jagħmlu din il-valutazzjoni fiż-żmien li jsiru jafu bil-ksur. Il-kontrollur ma għandux jistenna eżami forensiku dettaljat u passi ta' mitigazzjoni (bikrija) qabel ma jivvaluta jekk il-ksur tad-*data* huwiex probabbli li jirriżulta f'riskju u li għalhekk għandu jiġi nnotifikat.

10. Jekk kontrollur jivvaluta r-riskju huwa stess bħala improbabbli, iżda jirriżulta li r-riskju jimmaterjalizza, l-SA kompetenti tista' tuża s-setgħat korrettivi tagħha u tista' tiddeċiedi li timponi sanzjonijiet

11. Kull kontrollur u proċessur għandu jkollu pjanijiet u proċeduri stabbiliti għall-immaniġġar ta' ksur eventwali tad-*data*. L-organizzazzjonijiet għandu jkollhom linji ta' rapportar ċari u persuni responsabbli għal ċerti aspetti tal-proċess ta' rkupru.

12. It-taħriġ u s-sensibilizzazzjoni dwar kwistjonijiet ta' protezzjoni tad-*data* għall-persunal tal-kontrollur u tal-proċessur li jiffokaw fuq l-immaniġġar tal-ksur tad-*data* personali (l-identifikazzjoni ta' inċident ta' ksur ta' *data* personali u azzjonijiet ulterjuri li għandhom jittieħdu, eċċ.) huma essenzjali wkoll għall-kontrolluri u għall-proċessuri. Dan it-taħriġ għandu jiġi ripetut b'mod regolari, skont it-tip ta' attività ta' pproċessar u d-daqs tal-kontrollur, filwaqt li jiġu indirizzati l-aħħar xejriet u twissijiet li jkunu ġejjin miċ-ċiberattakki jew minn inċidenti ċibernetiċi oħrajn.

13. Il-prinċipju tal-akkontabilità u l-kunċett tal-protezzjoni tad-*data* mid-disinn jistgħu jinkorporaw analiżi li tikkontribwixxi għal "Manwal dwar l-Immaniġġar tal-Ksur tad-*Data* personali" tal-kontrollur tad-*data* u tal-proċessur tad-*data* stess li jkollu l-għan li jistabbilixxi fatti għal kull aspett tal-ipproċessar f'kull stadju ewlieni tal-operazzjoni. Manwal bħal dan imħejji minn qabel jipprovdi sors ta' informazzjoni ħafna aktar rapidu sabiex jippermetti lill-kontrolluri tad-*data* u lill-proċessuri tad-*data* jimmitigaw ir-riskji u jissodisfaw l-obbligi mingħajr dewmien żejjed. Dan jiżgura li jekk iseħħ ksur ta' *data* personali, in-nies fl-organizzazzjoni jkunu jafu x'għandhom jagħmlu, u l-inċident x'aktarx jiġi mmaniġġat aktar malajr milli kieku ma kien hemm l-ebda mitigazzjoni jew pjan stabbilit.

14. Għalkemm il-każijiet ippreżentati hawn taħt huma fittizji, huma bbażati fuq każijiet tipiċi mill-esperjenza kollettiva tal-SAs b'notifiki ta' ksur tad-*data*. L-analiżijiet offruti huma relatati b'mod espliċitu mal-każijiet taħt skrutinju, iżda bil-għan li jipprovdu assistenza lill-kontrolluri tad-*data* fil-valutazzjoni tal-ksur tad-*data* tagħhom stess. Kwalunkwe modifika fiċ-ċirkostanzi tal-każijiet deskritti hawn taħt tista' tirriżulta f'livelli ta' riskju differenti jew aktar sinifikanti, u b'hekk ikunu meħtieġa miżuri differenti jew addizzjonali. Dawn il-linji gwida jistrutturaw il-każijiet skont ċerti kategoriji ta' ksur (eż. attakki ransomware). Ċerti miżuri ta' mitigazzjoni huma mitluba f'kull każ meta tiġi ttrattata ċerta kategorija ta' ksur. Dawn il-miżuri ma humiex neċessarjament ripetuti f'kull analiżi tal-każ li tappartjeni għall-istess kategorija ta' ksur. Għall-każijiet li jappartjenu għall-istess kategorija huma stabbiliti biss id-differenzi. Għalhekk, il-qarrej għandu jaqra l-

[9] L-Artikolu 33(4) tal-GDPR.

każijiet kollha rilevanti għal kategorija rilevanti ta' ksur sabiex jidentifika u jiddistingwi l-miżuri korretti kollha li għandhom jittieħdu.

15. Id-dokumentazzjoni interna ta' ksur hija obbligu indipendenti mir-riskji marbuta mal-ksur, u trid titwettaq f'kull każ. Il-każijiet ippreżentati hawn taħt jipprovaw jitfgħu dawl fuq jekk il-ksur għandux jiġi nnotifikat lill-SA u jiġi kkomunikat lis-suġġetti tad-*data* affettwati.

2 RANSOMWARE

16. Kawża frekwenti għal notifika ta' ksur tad-*data* hija attakk ransomware li jġarrab il-kontrollur tad-*data*. F'dawn il-każijiet, kodiċi malizzjuż jikkripta d-*data* personali, u l-attakkant sussegwentement jitlob riskatt mingħand il-kontrollur bi skambju għall-kodiċi ta' dekriptaġġ. Dan it-tip ta' attakk jista' normalment jiġi kklassifikat bħala ksur tad-disponibbiltà, iżda spiss jista' jseħħ ukoll ksur tal-kunfidenzjalità.

2.1 KAŻ Nru 01: Ransomware b'kopja ta' riżerva xierqa u mingħajr eksfiltrazzjoni

Is-sistemi tal-kompjuter ta' kumpanija żgħira tal-manifattura ġew esposti għal attakk ransomware, u d-*data* maħżuna f'dawk is-sistemi kienet kriptata. Il-kontrollur tad-*data* uża l-kriptaġġ wieqaf, u għalhekk id-*data* kollha aċċessata mir-ransomware ġiet maħżuna f'forma kriptata bl-użu ta' algoritmu ta' kriptaġġ tal-ogħla livell ta' żvilupp tekniku. Il-kjavi tad-dekriptaġġ ma ġietx kompromessa fl-attakk, jiġifieri l-attakkant la seta' jaċċessaha u lanqas jużaha indirettament. B'konsegwenza ta' dan, l-attakkant kellu biss aċċess għal *data* personali kriptata. B'mod partikolari, la s-sistema tal-posta elettronika tal-kumpanija, u lanqas kwalunkwe sistema tal-klijenti użata sabiex din tiġi aċċessata ma ġew affettwati. Il-kumpanija qiegħda tuża l-għarfien espert ta' kumpanija esterna taċ-ċibersigurtà sabiex tinvestiga l-inċident. Il-log fajls li jittraċċaw il-flussi kollha tad-*data* li jħallu l-kumpanija (inkluża l-posta elettronika 'l barra) huma disponibbli. Wara li analizzat il-log fajls u d-*data* miġbura mis-sistemi ta' detezzjoni li nediet il-kumpanija, investigazzjoni interna appoġġata mill-kumpanija esterna taċ-ċibersigurtà ddeterminat *b'ċertezza* li l-awtur tar-reat biss ikkripta d-*data*, mingħajr ma jkun seraqha. Il-log fajls ma juru l-ebda fluss ta' *data* 'l barra fil-perjodu ta' żmien tal-attakk. Id-*data* personali affettwata mill-ksur hija relatata mal-klijenti u l-impjegati tal-kumpanija, ftit tużżani ta' individwi b'kollox. Kopja ta' riżerva kienet disponibbli faċilment, u d-*data* ġiet irrestawrata ftit sigħat wara li seħħ l-attakk. Il-ksur ma wassal għal ebda konsegwenza fuq l-operat ta' kuljum tal-kontrollur. Ma kien hemm l-ebda dewmien fil-pagamenti tal-impjegati jew fl-immaniġġar tat-talbiet tal-klijenti.

17. F'dan il-każ, l-elementi li ġejjin ġew irrealizzati mid-definizzjoni ta' "ksur ta' *data* personali": ksur tas-sigurtà wassal għal tibdil illegali u aċċess mhux awtorizzat għal *data* personali maħżuna.

2.1.1 KAŻ Nru 01 - Miżuri preventivi u valutazzjoni tar-riskju

18. Bħal fil-każ tar-riskji kollha maħluqa minn atturi esterni, il-probabbiltà li attakk ransomware jirnexxi tista' titnaqqas drastikament billi tiġi ristretta s-sigurtà tal-ambjent tal-kontroll tad-*data*. Il-maġġoranza ta' dawn il-każijiet ta' ksur tista' tiġi pprevenuta billi jiġi żgurat li jkunu ttieħdu miżuri ta' sigurtà organizzazzjonali, fiżiċi u teknoloġiċi xierqa. Eżempji ta' miżuri bħal dawn huma patch management xieraq u l-użu ta' sistema xierqa ta' detezzjoni kontra l-malware. Kopja ta' riżerva xierqa u separata tgħin sabiex jiġu mmitigati l-konsegwenzi ta' attakk b'suċċess f'każ li dan iseħħ. Barra minn hekk, programm ta' edukazzjoni, taħriġ u sensibilizzazzjoni dwar is-sigurtà tal-impjegati (SETA) se jgħin fil-prevenzjoni u r-rikonoxximent ta' dan it-tip ta' attakk. (Lista ta' miżuri rakkomandati tinsab fit-Taqsima 2.5.) Fost dawk il-miżuri, patch management xieraq li jiżgura li s-sistemi jkunu aġġornati u li l-vulnerabbiltajiet kollha magħrufa tas-sistemi użati jkunu fissi hija waħda mill-aktar importanti peress li l-biċċa l-kbira tal-attakki ransomware jisfruttaw vulnerabbiltajiet magħrufa sew.

19. Meta jivvaluta r-riskji, il-kontrollur għandu jinvestiga l-ksur u jidentifika t-tip ta' kodiċi malizzjuż sabiex jifhem il-konsegwenzi possibbli tal-attakk. Fost dawk ir-riskji li għandhom jiġu kkunsidrati hemm ir-riskju li d-*data* ġiet eksfiltrata mingħajr ma ħalliet traċċa fil-log fajls tas-sistemi.

20. F'dan l-eżempju, l-attakkant kellu aċċess għad-*data* personali u l-kunfidenzjalità tat-test ċifrat li fih *data* personali f'forma kriptata ġiet kompromessa. Madankollu, kwalunkwe *data* li setgħet ġiet eksfiltrata ma tistax tinqara jew tintuża mill-awtur tar-reat, tal-inqas għalissa. It-teknika ta' kriptaġġ użata mill-kontrollur tad-*data* tikkonforma mal-ogħla livell ta' żvilupp tekniku. Il-kjavi tad-dekriptaġġ ma kinitx kompromessa u preżumibbilment lanqas ma setgħet tiġi ddeterminata b'mezzi oħrajn. B'konsegwenza ta' dan, ir-riskji ta' kunfidenzjalità għad-drittijiet u l-libertajiet tal-persuni fiżiċi jitnaqqsu għall-minimu u jiġi eliminat il-progress kriptoanalitiku, li jagħmel id-*data* kriptata intelliġibbli fil-futur.

21. Il-kontrollur tad-*data* għandu jqis ir-riskju għall-individwi minħabba l-ksur[10]. F'dan il-każ, jidher li r-riskji għad-drittijiet u l-libertajiet tas-suġġetti tad-*data* jirriżultaw min-nuqqas ta' disponibbiltà tad-*data* personali, u l-kunfidenzjalità tad-*data* personali ma tiġix kompromessa[11]. F'dan l-eżempju, l-effetti negattivi tal-ksur ġew mitigati ftit wara li seħħ il-ksur. Il-fatt li jkun hemm kopja ta' riżerva xierqa[12] jagħmel l-effetti tal-ksur inqas gravi u hawnhekk il-kontrollur seta' jagħmel użu minnha b'mod effettiv.

22. Fir-rigward tas-severità tal-konsegwenzi għas-suġġetti tad-*data*, setgħu jiġu identifikati biss konsegwenzi żgħar peress li d-*data* affettwata ġiet irrestawrata fi ftit sigħat, il-ksur ma rriżulta fl-ebda konsegwenza fuq l-operat ta' kuljum tal-kontrollur u ma kellu l-ebda effett sinifikanti fuq is-suġġetti tad-*data* (eż. il-pagamenti tal-impjegati jew l-immaniġġar tat-talbiet tal-klijenti).

2.1.2 KAŻ Nru 01 – Mitigazzjoni u obbligi

23. Mingħajr kopja ta' riżerva jistgħu jittieħdu biss ftit miżuri sabiex jiġi rrimedjat it-telf ta' *data* personali mill-kontrollur, u d-*data* trid terġa' tinġabar. Madankollu, f'dan il-każ partikolari, l-impatti tal-attakk jistgħu jiġu kkontrollati b'mod effettiv billi s-sistemi kompromessi kollha jiġu ssettjati mill-ġdid għal stat nadif magħruf li huwa ħieles minn kodiċi malizzjuż, jiġu ffissati l-vulnerabbiltajiet u tiġi rrestawrata d-*data* affettwata ftit wara l-attakk. Mingħajr kopja ta' riżerva tintilef id-*data*, u s-severità tista' tiżdied minħabba r-riskji jew l-impatti fuq l-individwi.

---

[10] Għal gwida dwar operazzjonijiet ta' pproċessar li "*x'aktarx jirriżultaw f'riskju għoli*", ara l-"Linji Gwida dwar Valutazzjoni tal-Impatt fuq il-Protezzjoni tad-*Data* (DPIA) u d-determinazzjoni dwar jekk l-ipproċessar 'x'aktarx jirriżulta f'riskju għoli' għall-finijiet tar-Regolament 2016/679" tal-Grupp ta' Ħidma A29, WP248 rev. 01, - approvat mill-EDPB, https://ec.europa.eu/newsroom/article29/items/611236, p. 9.

[11] Teknikament, il-kriptaġġ tad-*data* jinvolvi "aċċess" għal *data* oriġinali, u fil-każ ta' ransomware, it-tħassir tal-oriġinali – id-*data* jeħtieġ li tiġi aċċessata permezz ta' kodiċi ta' ransomware sabiex tiġi kriptata, u sabiex titneħħa d-*data* oriġinali. Attakkant jista' jieħu kopja tal-oriġinali qabel it-tħassir, iżda d-*data* personali mhux dejjem tiġi estratta. Waqt li investigazzjoni tal-kontrollur tad-*data* timxi 'l quddiem, jista' jkun hemm informazzjoni ġdida li tibdel din il-valutazzjoni. Aċċess li jirriżulta f'qerda illegali, telf, alterazzjoni, żvelar mhux awtorizzat tad-*data* personali, jew f'riskju għas-sigurtà lil suġġett tad-*data*, anke mingħajr interpretazzjoni tad-*data* jista' jkun sever daqs aċċess bl-interpretazzjoni tad-*data* personali.

[12] Il-proċeduri tal-kopji ta' riżerva għandhom ikunu strutturati, konsistenti u ripetibbli. Eżempji ta' proċeduri tal-kopji ta' riżerva huma l-metodu 3-2-1 u l-metodu grandfather-father-son. Kwalunkwe metodu għandu dejjem jiġi ttestjat għall-effettività fil-kopertura u meta d-*data* għandha tiġi rrestawrata. L-ittestjar għandu jiġi ripetut ukoll f'intervalli u speċjalment meta jseħħu bidliet fl-operazzjoni tal-ipproċessar jew fiċ-ċirkostanzi tagħha sabiex tiġi żgurata l-integrità tas-sistema.

24. Ir-restawr effettiv u f'waqtu tad-*data* mill-kopja ta' riżerva disponibbli huwa varjabbli ewlieni meta jiġi analizzat il-ksur. L-ispeċifikazzjoni ta' perjodu ta' żmien xieraq għar-restawr tad-*data* kompromessa tiddependi miċ-ċirkostanzi uniċi tal-ksur inkwistjoni. Il-GDPR jiddikjara li ksur ta' *data* personali għandu jiġi nnotifikat mingħajr dewmien żejjed u, fejn fattibbli, mhux aktar tard minn 72 siegħa wara. Għalhekk, jista' jiġi ddeterminat li l-qbiż tal-limitu ta' żmien ta' 72 siegħa ma huwiex rakkomandabbli fi kwalunkwe każ, iżda meta jiġu ttrattati każijiet ta' livell għoli ta' riskju, anke l-konformità ma' din l-iskadenza tista' titqies bħala mhux sodisfaċenti.

25. F'dan il-każ, wara valutazzjoni tal-impatt dettaljata u proċess ta' rispons għall-inċidenti, il-kontrollur iddetermina li ma kienx probabbli li l-ksur jirriżulta f'riskju għad-drittijiet u l-libertajiet tal-persuni fiżiċi, u għalhekk ma hija meħtieġa l-ebda komunikazzjoni lis-suġġetti tad-*data*, u l-ksur lanqas ma jirrikjedi notifika lill-SA. Madankollu, bħal kull ksur tad-*data*, dan għandu jiġi ddokumentat f'konformità mal-Artikolu 33(5). L-organizzazzjoni tista' teħtieġ ukoll (jew aktar tard tkun meħtieġa mill-SA) li taġġorna u tirrimedja l-miżuri u l-proċeduri organizzazzjonali u tekniċi tagħha ta' mmaniġġar tas-sigurtà tad-*data* personali u ta' mitigazzjoni tar-riskju. Fil-qafas ta' dan l-aġġornament u r-rimedju, l-organizzazzjoni għandha tinvestiga bir-reqqa l-ksur u tidentifika l-kawżi u l-metodi użati mill-awtur tar-reat sabiex jiġu pprevenuti avvenimenti simili fil-futur.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	X	X

2.2 KAŻ Nru 02: Ransomware mingħajr kopja ta' riżerva xierqa

Wieħed mill-kompjuters użati minn kumpanija agrikola ġie espost għal attakk ransomware u d-*data* tiegħu ġiet kriptata mill-attakkant. Il-kumpanija qiegħda tuża l-għarfien espert ta' kumpanija esterna taċ-ċibersigurtà sabiex timmonitorja n-network tagħha. Il-log fajls li jittraċċaw il-flussi kollha tad-*data* li jħallu l-kumpanija (inkluża l-posta elettronika 'l barra) huma disponibbli. Wara l-analiżi tal-logs u tad-*data*, is-sistemi l-oħrajn ta' detezzjoni ġabru l-investigazzjoni interna megħjuna mill-kumpanija taċ-ċibersigurtà li ddeterminat li l-awtur tar-reat biss ikkripta d-*data*, mingħajr ma seraqha. Il-log fajls ma juru l-ebda fluss ta' *data* 'l barra fil-perjodu ta' żmien tal-attakk. Id-*data* personali affettwata mill-ksur hija relatata mal-impjegati u l-klijenti tal-kumpanija, ftit tużżani ta' individwi b'kollox. Ma ġiet affettwata l-ebda kategorija speċjali ta' *data*. L-ebda kopja ta' riżerva ma kienet disponibbli f'forma elettronika. Il-biċċa l-kbira tad-*data* ġiet irrestawrata mill-kopji ta' riżerva stampati. Ir-restawr tad-*data* ħa ħamest ijiem ta' xogħol u wassal għal dewmien minuri fil-konsenja tal-ordnijiet lill-klijenti.

2.2.1 KAŻ Nru 02 - Miżuri preventivi u valutazzjoni tar-riskju

26. Il-kontrollur tad-*data* għandu jkun adotta l-istess miżuri preventivi kif imsemmi fil-parti 2.1. u fit-Taqsima 2.9. Id-differenza ewlenija f'dan il-każ meta mqabbel mal-każ preċedenti hija n-nuqqas ta' kopja ta' riżerva elettronika u n-nuqqas ta' kriptaġġ wieqaf. Dan iwassal għal differenzi kritiċi fil-passi segwenti.

27. Meta jivvaluta r-riskji, il-kontrollur għandu jinvestiga l-metodu ta' infiltrazzjoni u jidentifika t-tip ta' kodiċi malizzjuż sabiex jifhem il-konsegwenzi possibbli tal-attakk. F'dan l-eżempju, ir-ransomware ikkripta d-*data* personali mingħajr ma eksfiltraha. B'riżultat ta' dan, jidher li r-riskji għad-drittijiet u l-libertajiet tas-suġġetti tad-*data* jirriżultaw min-nuqqas ta' disponibbiltà tad-*data* personali, u l-kunfidenzjalità tad-*data* personali ma hijiex kompromessa. Eżami bir-reqqa tal-logs tal-firewall u l-implikazzjonijiet tiegħu huma essenzjali sabiex jiġi ddeterminat ir-riskju. Il-kontrollur tad-*data* għandu jippreżenta s-sejbiet fattwali ta' dawn l-investigazzjonijiet fuq talba.

28. Il-kontrollur tad-*data* jeħtieġ li jżomm f'moħħu li jekk l-attakk ikun aktar sofistikat, il-malware għandu l-funzjonalità li jeditja l-log fajls u jneħħi t-traċċa. Għalhekk - minħabba li l-logs ma jintbagħtux jew jiġu replikati lil server ċentrali tal-logs - anke wara investigazzjoni bir-reqqa li ddeterminat li d-*data* personali ma kinitx ġiet eksfiltrata mill-attakkant, il-kontrollur tad-*data* ma jistax jiddikjara li n-nuqqas ta' entrata ta' log jagħti prova tan-nuqqas ta' eksfiltrazzjoni, għalhekk, il-probabbiltà ta' ksur ta' kunfidenzjalità ma tistax tiġi miċħuda kompletament.

29. Il-kontrollur tad-*data* għandu jivvaluta r-riskji ta' dan il-ksur[13] jekk id-*data* tkun ġiet aċċessata mill-attakkant. Matul il-valutazzjoni tar-riskju, il-kontrollur tad-*data* għandu jqis ukoll in-natura, is-sensittività, il-volum, u l-kuntest tad-*data* personali affettwata fil-ksur. F'dan il-każ ma hija affettwata l-ebda kategorija speċjali ta' *data* personali, u l-kwantità ta' *data* li fuqha tkun seħħet vjolazzjoni u n-numru ta' suġġetti tad-*data* affettwati huma baxxi.

30. Il-ġbir ta' informazzjoni eżatta dwar l-aċċess mhux awtorizzat huwa kruċjali sabiex jiġi ddeterminat il-livell ta' riskju u sabiex jiġi evitat attakk ġdid jew kontinwu. Li kieku d-*data* ġiet ikkopjata mill-bażi ta' *data*, dan kien ovvjament ikun fattur li jżid ir-riskju. Meta ma jkunx hemm ċertezza dwar l-ispeċifiċitajiet tal-aċċess illeġittimu, għandu jiġi kkunsidrat l-agħar xenarju u r-riskju għandu jiġi vvalutat kif xieraq.

31. In-nuqqas ta' bażi ta' *data* ta' kopja ta' riżerva jista' jitqies bħala fattur li jżid ir-riskju skont is-severità tal-konsegwenzi għas-suġġetti tad-*data* li jirriżultaw min-nuqqas ta' disponibbiltà tad-*data*.

2.2.2 KAŻ Nru 02 – Mitigazzjoni u obbligi

32. Mingħajr kopja ta' riżerva jistgħu jittieħdu biss ftit miżuri sabiex jiġi rrimedjat it-telf ta' *data* personali mill-kontrollur, u d-*data* trid terġa' tinġabar, sakemm ma jkunx disponibbli xi sors ieħor (eż. il-posta elettronika relatata mal-konfermi tal-ordnijiet). Mingħajr kopja ta' riżerva, id-*data* tista' tintilef u s-severità tkun tiddependi fuq l-impatt għall-individwi.

33. Ir-restawr tad-*data* ma għandux ikun problematiku żżejjed[14] jekk id-*data* tkun għadha disponibbli fuq format stampat, iżda minħabba n-nuqqas ta' bażi ta' *data* elettronika ta' kopja ta' riżerva, titqies meħtieġa notifika lill-SA, peress li r-restawr tad-*data* jkun ħa xi żmien u jista' jikkawża xi dewmien fil-konsenja tal-ordnijiet lill-klijenti u jista' ma jkunx jista' jiġi rkuprat ammont konsiderevoli ta' metadata (eż. logs, kronogrammi).

34. L-għoti ta' informazzjoni lis-suġġetti tad-*data* dwar il-ksur jista' jiddependi wkoll fuq it-tul ta' żmien li d-*data* personali ma tkunx disponibbli u d-diffikultajiet li dan jista' jikkawża fl-operat tal-kontrollur bħala riżultat (eż. dewmien fit-trasferiment tal-pagamenti tal-impjegati). Peress li dan id-dewmien fil-pagamenti u fil-konsenji jista' jwassal għal telf finanzjarju għall-individwi li d-*data* tagħhom tkun ġiet kompromessa, wieħed jista' jsostni wkoll li l-ksur x'aktarx li jirriżulta f'riskju għoli. Barra minn hekk, jista' ma jkunx possibbli li jiġi evitat li s-suġġetti tad-*data* jiġu informati jekk il-kontribuzzjoni tagħhom tkun meħtieġa għar-restawr tad-*data* kriptata.

35. Dan il-każ iservi bħala eżempju ta' attakk ransomware b'riskju għad-drittijiet u l-libertajiet tas-suġġetti tad-*data*, iżda li ma jilħaqx riskju għoli. Dan għandu jiġi ddokumentat f'konformità mal-Artikolu 33(5) u nnotifikat

---

[13] Għal gwida dwar operazzjonijiet ta' pproċessar li "*x'aktarx jirriżultaw f'riskju għoli*", ara n-nota 10 f'qiegħ il-paġna hawn fuq.

[14] Dan ikun jiddependi fuq il-kumplessità u l-istruttura tad-*data* personali. Fl-aktar xenarji kumplessi, l-istabbiliment mill-ġdid tal-integrità tad-*data*, il-konsistenza mal-metadata, l-iżgurar ta' relazzjonijiet korretti fi ħdan l-istrutturi tad-*data* u l-verifika tal-preċiżjoni tad-*data* jistgħu jeħtieġu riżorsi u sforz sinifikanti.

lill-SA f'konformità mal-Artikolu 33(1). L-organizzazzjoni tista' teħtieġ ukoll (jew aktar tard tkun meħtieġa mill-SA) li taġġorna u tirrimedja l-miżuri u l-proċeduri organizzazzjonali u tekniċi tagħha ta' mmaniġġar tas-sigurtà tad-*data* personali u ta' mitigazzjoni tar-riskju.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	✓	X

2.3 KAŻ Nru 03: Ransomware b'kopja ta' riżerva u mingħajr eksfiltrazzjoni fi sptar

Is-sistema ta' informazzjoni ta' sptar/ċentru ta' kura tas-saħħa kienet esposta għal attakk ransomware u proporzjon sinifikanti tad-*data* tagħha kien kriptat mill-attakkant. Il-kumpanija qiegħda tuża l-għarfien espert ta' kumpanija esterna taċ-ċibersigurtà sabiex timmonitorja n-network tagħha. Il-log fajls li jittraċċaw il-flussi kollha tad-*data* li jħallu l-kumpanija (inkluża l-posta elettronika 'l barra) huma disponibbli. Wara l-analiżi tal-log fajls u tad-*data*, is-sistemi l-oħrajn ta' detezzjoni ġabru l-investigazzjoni interna megħjuna mill-kumpanija taċ-ċibersigurtà li ddeterminat li l-awtur tar-reat biss ikkripta d-*data*, mingħajr ma seraqha. Il-log fajls ma juru l-ebda fluss ta' *data* 'l barra fil-perjodu ta' żmien tal-attakk. Id-*data* personali affettwata mill-ksur hija relatata mal-impjegati u l-pazjenti, li rrappreżentaw eluf ta' individwi. Il-kopji ta' riżerva kienu disponibbli f'format elettroniku. Il-biċċa l-kbira tad-*data* ġiet irrestawrata iżda din l-operazzjoni ħadet jumejn ta' xogħol u wasslet għal dewmien kbir fit-trattament tal-pazjenti minħabba l-ikkanċellar/l-posponiment tal-operazzjonijiet kirurġiċi, u għal tnaqqis fil-livell tas-servizz minħabba n-nuqqas ta' disponibbiltà tas-sistemi.

2.3.1 KAŻ Nru 03 - Miżuri preventivi u valutazzjoni tar-riskju

36. Il-kontrollur tad-*data* għandu jkun adotta l-istess miżuri preventivi kif imsemmi fil-parti 2.1. u fit-Taqsima 2.5. Id-differenza ewlenija f'dan il-każ meta mqabbel mal-każ preċedenti hija l-livell għoli ta' severità tal-konsegwenzi għal parti sostanzjali tas-suġġetti tad-*data*[15].

37. Il-kwantità ta' *data* li fuqha tkun seħħet vjolazzjoni u n-numru ta' suġġetti tad-*data* affettwati huma għoljin, minħabba li l-isptarijiet normalment jipproċessaw kwantitajiet kbar ta' *data*. In-nuqqas ta' disponibbiltà tad-*data* għandu impatt kbir fuq parti sostanzjali mis-suġġetti tad-*data*. Barra minn hekk, hemm riskju residwu ta' livelll għoli ta' severità għall-kunfidenzjalità tad-*data* tal-pazjent.

38. It-tip ta' ksur, in-natura, is-sensittività u l-volum ta' *data* personali affettwati fil-ksur huma importanti. Minkejja li kienet teżisti kopja ta' riżerva tad-*data* u din setgħet tiġi rrestawrata fi ftit jiem, jeżisti riskju għoli

[15] Għal gwida dwar operazzjonijiet ta' pproċessar li "*x'aktarx jirriżultaw f'riskju għoli*", ara n-nota 10 f'qiegħ il-paġna hawn fuq.

minħabba s-severità tal-konsegwenzi għas-suġġetti tad-*data* li jirriżultaw min-nuqqas ta' disponibbiltà tad-*data* fil-mument tal-attakk u fil-jiem ta' wara.

2.3.2 KAŻ Nru 03 – Mitigazzjoni u obbligi

39. Notifika lill-SA hija meqjusa neċessarja, peress li huma involuti kategoriji speċjali ta' *data* personali u r-restawr tad-*data* jista' jieħu żmien twil, li jirriżulta f'dewmien kbir fil-kura tal-pazjenti. L-għoti ta' informazzjoni lis-suġġetti tad-*data* dwar il-ksur huwa meħtieġ minħabba l-impatt għall-pazjenti, anke wara li tiġi rrestawrata d-*data* kriptata. Filwaqt li d-*data* relatata mal-pazjenti kollha ttrattati fl-isptar matul l-aħħar snin kienet kriptata, kienu biss dawk il-pazjenti li kienu skedati li jiġu ttrattati fl-isptar matul iż-żmien li fih is-sistema tal-kompjuter ma kinitx disponibbli li ntlaqtu. Il-kontrollur għandu jikkomunika l-ksur tad-*data* direttament lil dawk il-pazjenti. Komunikazzjoni diretta lill-pazjenti l-oħrajn li whud minnhom setgħu ma daħlux l-isptar għal aktar minn għoxrin sena tista' ma tkunx meħtieġa minħabba l-eċċezzjoni fl-Artikolu 34(3) c). F'każ bħal dan, minflok għandu jkun hemm komunikazzjoni pubblika[16] jew miżura simili li fiha s-suġġetti tad-*data* jiġu informati b'mod ugwalment effettiv. F'dan il-każ, l-isptar għandu jagħmel l-attakk ransomware u l-effetti tiegħu pubbliċi.

40. Dan il-każ iservi bħala eżempju ta' attakk ransomware b'riskju għoli għad-drittijiet u l-libertajiet tas-suġġetti tad-*data*. Dan għandu jiġi ddokumentat f'konformità mal-Artikolu 33(5), innotifikat lill-SA f'konformità mal-Artikolu 33(1) u kkomunikat lis-suġġetti tad-*data* f'konformità mal-Artikolu 34(1). L-organizzazzjoni jeħtieġ ukoll li taġġorna u tirrimedja l-miżuri u l-proċeduri organizzazzjonali u tekniċi tagħha ta' mmaniġġar tas-sigurtà tad-*data* personali u ta' mitigazzjoni tar-riskju.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	✓	✓

2.4 KAŻ Nru 04: Ransomware mingħajr kopja ta' riżerva u b'eksfiltrazzjoni

Is-server ta' kumpanija tat-trasport pubbliku ġie espost għal attakk ta' ransomware u d-*data* tiegħu ġiet kriptata mill-attakkant. Skont is-sejbiet tal-investigazzjoni interna, l-awtur tar-reat mhux biss ikkripta d-*data*, iżda wkoll eksfiltraha. It-tip ta' *data* li fuqha tkun seħħet vjolazzjoni kienet id-*data* personali tal-klijenti u tal-impjegati, u l-eluf ta' persuni li jużaw is-servizzi tal-kumpanija (eż. meta jinxtraw il-biljetti online). Lil hinn minn *data* tal-identità bażika, numri ta' karti tal-identità u *data* finanzjarja bħal dettalji ta' karti ta' kreditu huma involuti fil-ksur. Kienet teżisti kopja ta' riżerva tal-bażi ta' *data*, iżda kienet kriptata wkoll mill-attakkant.

[16] Il-Premessa 86 tal-GDPR tispjega li "*tali komunikazzjonijiet lis-suġġetti tad-data għandhom isiru malajr kemm jista' jkun raġonevolment fattibbli u f'kooperazzjoni mill-qrib mal-awtorità superviżorja, b'mod li jirrispetta l-gwida mogħtija minnha jew minn awtoritajiet rilevanti oħrajn, bħal awtoritajiet tal-infurzar tal-liġi. Pereżempju, il-bżonn li jitnaqqas riskju immedjat ta' dannu jitlob komunikazzjoni immedjata mas-suġġetti tad-data filwaqt li l-ħtieġa li jiġu implimentati miżuri adatti kontra każijiet kontinwi jew simili ta' vjolazzjoni ta' data personali tista' tiġġustifika żmien itwal għal komunikazzjoni*".

2.4.1 KAŻ Nru 04 - Miżuri preventivi u valutazzjoni tar-riskju

41. Il-kontrollur tad-*data* għandu jkun adotta l-istess miżuri preventivi kif imsemmi fil-parti 2.1. u fit-Taqsima 2.5. Għalkemm kien hemm kopja ta' riżerva stabbilita, din ġiet affettwata wkoll mill-attakk. Dan l-arranġament waħdu jqajjem mistoqsijiet dwar il-kwalità tal-miżuri preċedenti ta' sigurtà tal-IT tal-kontrollur u għandu jiġi skrutinizzat aktar matul l-investigazzjoni, peress li f'sistema ta' kopja ta' riżerva mfassla tajjeb, iridu jinħażnu diversi kopji ta' riżerva b'mod sigur mingħajr aċċess mis-sistema ewlenija, inkella jistgħu jiġu kompromessi fl-istess attakk. Barra minn hekk, l-attakki ransomware jistgħu ma jinkixfux għal numru ta' ġranet meta tkun qiegħda tiġi kriptata *data* li tintuża rarament. Dan jista' jagħmel id-diversi kopji ta' riżerva inutli, għalhekk il-kopji ta' riżerva għandhom ukoll jittieħdu perjodikament u jiġu iżolati. Dan iżid il-probabbiltà ta' rkupru għalkemm b'telf ta' *data* akbar.

42. Dan il-ksur jikkonċerna mhux biss id-disponibbiltà tad-*data*, iżda wkoll il-kunfidenzjalità, peress li l-attakkant jista' jkun immodifika u/jew ikkopja d-*data* mis-server. Għalhekk, it-tip ta' ksur jirriżulta f'riskju għoli[17].

43. In-natura, is-sensittività u l-volum ta' *data* personali jkomplu jżidu r-riskji, minħabba li n-numru ta' individwi affettwati huwa għoli, bħalma hija l-kwantità globali ta' *data* personali affettwata. Lil hinn minn *data* tal-identità bażika, huma involuti wkoll dokumenti tal-identità u *data* finanzjarja bħal dettalji ta' karti ta' kreditu. Ksur ta' *data* li jikkonċerna dawn it-tipi ta' *data* jippreżenta riskju għoli fih u minnu nnifsu, u jekk dawn jiġu pproċessati flimkien, jistgħu jintużaw għal – fost l-oħrajn – serq tal-identità jew frodi.

44. Minħabba l-loġika tas-server difettuża jew il-kontrolli organizzazzjonali, il-fajls tal-kopji ta' riżerva ġew affettwati mir-ransomware, u dan ipprevjena r-restawr tad-*data* u kabbar ir-riskju.

45. Dan il-ksur tad-*data* jippreżenta riskju għoli għad-drittijiet u l-libertajiet tal-individwi, minħabba li x'aktarx jista' jwassal għal ħsara kemm materjali (eż. telf finanzjarju peress li ġew affettwati dettalji ta' karti ta' kreditu) kif ukoll mhux materjali (eż. serq tal-identità jew frodi peress li ġew affettwati dettalji ta' karti tal-identità).

2.4.2 KAŻ Nru 04 – Mitigazzjoni u obbligi

46. Il-komunikazzjoni lis-suġġetti tad-*data* hija essenzjali, sabiex ikunu jistgħu jieħdu l-passi meħtieġa sabiex jevitaw ħsara materjali (eż. jimblukkaw il-karti ta' kreditu tagħhom).

47. Minbarra d-dokumentazzjoni tal-ksur f'konformità mal-Artikolu 33(5), notifika lill-SA hija obbligatorja wkoll f'dan il-każ (l-Artikolu 33(1)) u l-kontrollur huwa obbligat ukoll jikkomunika l-ksur lis-suġġetti tad-*data* (l-Artikolu 34(1)). Dan tal-aħħar jista' jsir fuq bażi ta' persuna b'persuna, iżda għal individwi fejn id-*data* ta' kuntatt ma tkunx disponibbli, il-kontrollur għandu jagħmel dan b'mod pubbliku, dment li tali komunikazzjoni ma tkunx suxxettibbli li tiskatta konsegwenzi negattivi addizzjonali għas-suġġetti tad-*data*, eż. permezz ta' notifika fuq is-sit web tiegħu. F'dan l-aħħar każ hija meħtieġa komunikazzjoni preċiża u ċara, b'mod ċar fuq il-paġna ewlenija tal-kontrollur, b'referenzi eżatti għad-dispożizzjonijiet rilevanti tal-GDPR. L-organizzazzjoni tista' wkoll teħtieġ li taġġorna u tirrimedja l-miżuri u l-proċeduri organizzazzjonali u tekniċi tagħha ta' mmaniġġar tas-sigurtà tad-*data* personali u ta' mitigazzjoni tar-riskju.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*

[17] Għal gwida dwar operazzjonijiet ta' pproċessar li "*x'aktarx jirriżultaw f'riskju għoli*", ara n-nota 10 f'qiegħ il-paġna hawn fuq.

✓	✓	✓

2.5 Miżuri organizzazzjonali u tekniċi għall-prevenzjoni/għall-mitigazzjoni tal-impatti tal-attakki ransomware

48. Il-fatt li seta' seħħ attakk ransomware huwa normalment sinjal ta' vulnerabbiltà waħda jew aktar fis-sistema tal-kontrollur. Dan japplika wkoll f'każijiet ta' ransomware li fihom tkun ġiet kriptata d-*data* personali, iżda ma tkunx ġiet eksfiltrata. Irrispettivament mill-eżitu u l-konsegwenzi tal-attakk, l-importanza ta' evalwazzjoni komprensiva tas-sistema tas-sigurtà tad-*data* - b'enfasi partikolari fuq is-sigurtà tal-IT - ma tistax tiġi enfasizzata biżżejjed. Id-dgħufijiet u l-kwistjonijiet ta' sigurtà identifikati għandhom jiġu ddokumentati u indirizzati mingħajr dewmien.

49. Miżuri rakkomandati:

(Il-lista tal-miżuri li ġejjin bl-ebda mod ma hija esklużiva jew komprensiva. Pjuttost, l-għan huwa li jiġu pprovduti ideat għall-prevenzjoni u soluzzjonijiet possibbli. Kull attività ta' proċessar hija differenti, għalhekk il-kontrollur għandu jieħu d-deċiżjoni dwar liema miżuri huma l-aktar adatti għas-sitwazzjoni partikolari.)

- L-aġġornament tal-firmware, tas-sistema operattiva u tas-software ta' applikazzjoni fuq is-servers, tal-magni tal-klijenti, tal-komponenti attivi tan-network, u ta' kwalunkwe magna oħra fl-istess LAN (inkluż l-apparat tal-Wi-Fi). L-iżgurar li jkunu stabbiliti miżuri xierqa ta' sigurtà tal-IT, filwaqt li jiġi żgurat li dawn ikunu effettivi u li jinżammu aġġornati b'mod regolari meta jinbidlu jew jevolvu l-ipproċessar jew iċ-ċirkostanzi. Dan jinkludi ż-żamma ta' log fajls dettaljati ta' liema patches jiġu applikati f'kronogramma partikolari.
- It-tfassil u l-organizzazzjoni ta' sistemi ta' pproċessar u infrastruttura għat-tqassim jew l-iżolament ta' sistemi u networks tad-*data* sabiex tiġi evitata l-propagazzjoni ta' malware fl-organizzazzjoni u f'sistemi esterni.
- L-eżistenza ta' proċedura ta' kopja ta' riżerva aġġornata, sigura u ttestjata. Kopji ta' riżerva ta' media għal perjodi ta' żmien medji u twal għandhom jinżammu separati mill-ħżin ta' *data* operazzjonali u jinżammu fejn ma jkunux jistgħu jintlaħqu minn partijiet terzi anke f'każ ta' attakk li jirnexxi (bħal kopji ta' riżerva inkrimentali ta' kuljum u kopji ta' riżerva sħaħ li jsiru kull ġimgħa).
- Li jkollhom/jiksbu software xieraq aġġornat, effettiv u integrat kontra l-malware.
- Li jkollhom sistema xierqa, aġġornata, effettiva u integrata tal-firewall u tad-detezzjoni u l-prevenzjoni tal-intrużjonijiet. Li jidderieġu t-traffiku tan-network permezz ta' firewall/tad-detezzjoni tal-intrużjoni, anke fil-każ ta' uffiċċju fid-dar jew xogħol mobbli (eż. billi jużaw konnessjonijiet VPN għal mekkaniżmi ta' sigurtà organizzazzjonali meta jaċċessaw l-internet).
- It-taħriġ tal-impjegati dwar il-metodi ta' rikonoxximent u ta' prevenzjoni tal-attakki tal-IT. Il-kontrollur għandu jipprovdi mezzi sabiex jiġi stabbilit jekk il-posta elettronika u l-messaġġi miksuba b'mezzi oħrajn ta' komunikazzjoni humiex awtentiċi u affidabbli. L-impjegati għandhom jiġu mħarrġa sabiex jirrikonoxxu meta jkun seħħ attakk bħal dan, dwar kif għandhom joħorġu l-punt ta' tmiem tan-network u dwar l-obbligu tagħhom li jirrapportaw minnufih lill-uffiċjal tas-sigurtà.
- Li tiġi enfasizzata l-ħtieġa li jiġi identifikat it-tip ta' kodiċi malizzjuż sabiex wieħed jara l-konsegwenzi tal-attakk u jkun jista' jidentifika l-miżuri t-tajba sabiex jimmitiga r-riskju. F'każ li attakk ransomware ikun irnexxa u ma jkun hemm l-ebda kopja ta' riżerva disponibbli, jistgħu jiġu applikati għodod disponibbli bħal dawk mill-proġett "no more ransom" (nomoreransom.org) sabiex tiġi rkuprata d-*data*. Madankollu, f'każ li jkun hemm kopja ta' riżerva sikura disponibbli, huwa rrakkomandat li d-*data* tiġi rrestawrata minnha.
- It-trażmissjoni jew ir-replikazzjoni tal-logs kollha fuq server ċentrali tal-log fajls (li possibbilment jinkludi l-iffirmar jew l-istampar tal-ħin kriptografiku tal-entrati tal-log fajl).

- Kriptaġġ b'saħħtu u awtentikazzjoni b'diversi fatturi, b'mod partikolari għall-aċċess amministrattiv għas-sistemi tal-IT, u l-immaniġġar xieraq tal-kjavi u l-passwords.
- L-ittestjar tal-vulnerabbiltà u tal-penetrazzjoni fuq bażi regolari.
- L-istabbiliment ta' Skwadra ta' Rispons għal Inċidenti relatati mas-Sigurtà tal-Kompjuters (CSIRT) jew Skwadra ta' Rispons f'Emerġenza relatata mal-Kompjuter (CERT) fi ħdan l-organizzazzjoni, jew sħubija f'CSIRT/CERT kollettiva. Il-ħolqien ta' Pjan ta' Rispons għall-Inċidenti, Pjan ta' Rkupru minn Diżastri u Pjan għall-Kontinwità tan-Negozju, filwaqt li jiġi żgurat li dawn jiġu ttestjati bir-reqqa.
- Meta jiġu vvalutati l-kontromiżuri – l-analiżi tar-riskju għandha tiġi rieżaminata, ittestjata u aġġornata.

3 ATTAKKI TA' EKSFILTRAZZJONI TAD-*DATA*

50. Attakki li jisfruttaw il-vulnerabbiltajiet fis-servizzi offruti mill-kontrollur lil partijiet terzi permezz tal-internet, eż. imwettqa permezz ta' attakki ta' injezzjoni (eż. l-injezzjoni SQL, it-traversa tal-mogħdija), il-kompromissjoni ta' sit web u l-metodi simili, jistgħu jixbhu l-attakki ransomware minħabba li r-riskju jirriżulta mill-azzjoni ta' parti terza mhux awtorizzata, iżda dawk l-attakki tipikament għandhom l-għan li jikkopjaw, jeksfiltraw u jabbużaw minn *data* personali għal xi fini malizzjuża. Għalhekk, huma prinċipalment ksur tal-kunfidenzjalità u, possibbilment, anke tal-integrità tad-*data*. Fl-istess ħin, jekk il-kontrollur ikun jaf dwar il-karatteristiċi ta' dan it-tip ta' ksur, hemm ħafna miżuri disponibbli għall-kontrolluri li jistgħu jnaqqsu b'mod sostanzjali r-riskju ta' eżekuzzjoni ta' attakk b'suċċess.

3.1 KAŻ Nru 05: Eksfiltrazzjoni ta' *data* relatata ma' applikazzjonijiet għax-xogħol minn sit web

Aġenzija tal-impjiegi kienet il-vittma ta' attakk ċibernetiku, li poġġa kodiċi malizzjuż fuq is-sit web tagħha. Dan il-kodiċi malizzjuż għamel l-informazzjoni personali sottomessa permezz ta' formoli ta' applikazzjoni għal xogħol online u maħżuna fuq is-server tal-web aċċessibbli għal persuna(i) mhux awtorizzata(i). 213-il formola bħal dawn huma possibbilment affettwati, wara li ġiet analizzata d-*data* affettwata, ġie ddeterminat li l-ebda kategorija speċjali ta' *data* ma ġiet affettwata fil-ksur. Is-sett ta' għodod tal-malware partikolari installat kellu funzjonalitajiet li ppermettew lill-attakkant ineħħi kwalunkwe storja ta' eksfiltrazzjoni u ppermetta wkoll li l-ipproċessar fuq is-server jiġi mmonitorjat u li tinkiseb id-*data* personali miġbura. Is-sett ta' għodod ġie skopert biss xahar wara l-installazzjoni tiegħu.

3.1.1 KAŻ Nru 05 - Miżuri preventivi u valutazzjoni tar-riskju

51. Is-sigurtà tal-ambjent tal-kontrollur tad-*data* hija estremament importanti, peress li l-maġġoranza ta' dawn il-każijiet ta' ksur tista' tiġi pprevenuta billi jiġi żgurat li s-sistemi kollha jiġu aġġornati b'mod kostanti, li *data* sensittiva tiġi kriptata u li l-applikazzjonijiet jiġu żviluppati skont standards ta' sigurtà għoljin bħal awtentikazzjoni b'saħħitha, miżuri kontra l-forza brutali, attakki, "il-ħrib" jew "is-sanitizzazzjoni"[18] tal-input tal-utenti, eċċ. Huma meħtieġa wkoll awditi perjodiċi tas-sigurtà tal-IT, valutazzjonijiet tal-vulnerabbiltà u testijiet tal-penetrazzjoni sabiex dawn it-tipi ta' vulnerabbiltajiet jiġu identifikati minn qabel u solvuti. F'dan il-każ partikolari, l-għodod ta' monitoraġġ tal-integrità tal-fajls fl-ambjent tal-produzzjoni setgħu għenu sabiex tiġi identifikata l-injezzjoni tal-kodiċi. (Lista ta' miżuri rakkomandati tinsab fit-Taqsima 3.7).

[18] Il-ħrib jew is-sanitizzazzjoni tal-inputs tal-utenti huma forma ta' validazzjoni tal-input, li tiżgura li tiddaħħal biss *data* fformalizzata kif suppost f'sistema ta' informazzjoni.

52. Il-kontrollur għandu dejjem jibda jinvestiga l-ksur billi jidentifika t-tip ta' attakk u l-metodi tiegħu, sabiex jivvaluta liema miżuri għandhom jittieħdu. Sabiex jagħmel dan malajr u b'mod effiċjenti, il-kontrollur tad-*data* għandu jkollu pjan ta' rispons għall-inċidenti stabbilit li jispeċifika l-passi rapidi u meħtieġa sabiex jieħu kontroll tal-inċident. F'dan il-każ partikolari, it-tip ta' ksur kien fattur li jżid ir-riskju peress li mhux biss kienet ristretta l-kunfidenzjalità tad-*data*, iżda l-infiltratur kellu wkoll il-mezzi sabiex jistabbilixxi bidliet fis-sistema, u għalhekk l-integrità tad-*data* saret dubjuża.

53. In-natura, is-sensittività u l-volum tad-*data* personali affettwata fil-ksur għandhom jiġu vvalutati sabiex jiġi ddeterminat sa liema punt il-ksur affettwa s-suġġetti tad-*data*. Għalkemm ma ġiet affettwata l-ebda kategorija speċjali ta' *data* personali, id-*data* aċċessata fiha informazzjoni konsiderevoli dwar l-individwi mill-formoli online, u tali *data* tista' tintuża ħażin b'għadd ta' modi (għall-immirar ta' kummerċjalizzazzjoni mhux mitluba, serq tal-identità, eċċ.), għalhekk is-severità tal-konsegwenzi għandha żżid ir-riskju għad-drittijiet u l-libertajiet tas-suġġetti tad-*data*[19].

3.1.2 KAŻ Nru 05 – Mitigazzjoni u obbligi

54. Jekk ikun possibbli, wara li tiġi solvuta l-problema, il-bażi ta' *data* għandha titqabbel ma' dik maħżuna f'kopja ta' riżerva sigura. L-esperjenzi li jirriżultaw mill-ksur għandhom jintużaw fl-aġġornament tal-infrastruttura tal-IT. Il-kontrollur tad-*data* għandu jirritorna s-sistemi tal-IT affettwati kollha għal stat nadif magħruf, jirrimedja l-vulnerabbiltà u jimplimenta miżuri ta' sigurtà ġodda sabiex jiġi evitat ksur tad-*data* simili fil-futur, eż. kontrolli tal-integrità tal-fajls u awditi tas-sigurtà. Jekk id-*data* personali ma ġietx biss eksfiltrata, iżda tħassret ukoll, il-kontrollur irid jieħu azzjoni sistematika sabiex jirkupra d-*data* personali fl-istat li kienet fih qabel il-ksur. Jista' jkun meħtieġ li jiġu applikati kopji ta' riżerva sħaħ, bidliet inkrementali u mbagħad possibbilment jerġa' jsir l-ipproċessar mill-aħħar kopja ta' riżerva inkrementali – li jirrikjedi li l-kontrollur ikun jista' jirreplika l-bidliet li saru mill-aħħar kopja ta' riżerva li tkun saret. Dan jista' jirrikjedi li l-kontrollur ikollu s-sistema mfassla sabiex iżomm il-fajls tal-input ta' kuljum f'każ li jkun hemm bżonn li jiġu pproċessati mill-ġdid u jirrikjedi metodu robust ta' ħżin u politika xierqa dwar iż-żamma.

55. Fid-dawl ta' dan ta' hawn fuq, peress li l-ksur x'aktarx li jirriżulta f'riskju għoli għad-drittijiet u l-libertajiet tal-persuni fiżiċi, is-suġġetti tad-*data* għandhom jiġu informati dwaru b'mod definittiv (l-Artikolu 34(1)), li naturalment, ifisser li l-SA(s) rilevanti għandhom ukoll ikunu involuti fil-forma ta' notifika ta' ksur ta' *data*. Id-dokumentazzjoni tal-ksur hija obbligatorja skont l-Artikolu 33(5) tal-GDPR u tagħmel il-valutazzjoni tas-sitwazzjoni aktar faċli.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	✓	✓

3.2 KAŻ Nru 06: Eksfiltrazzjoni ta' password hashed minn sit web

[19] Għal gwida dwar operazzjonijiet ta' pproċessar li "*x'aktarx jirriżultaw f'riskju għoli*", ara n-nota 10 f'qiegħ il-paġna hawn fuq.

Ġiet sfruttata vulnerabbiltà ta' injezzjoni SQL sabiex jinkiseb aċċess għal bażi ta' *data* tas-server ta' sit web tat-tisjir. L-utenti setgħu jagħżlu biss psewdonimi arbitrarji bħala identifikaturi tal-utent. L-użu ta' indirizzi tal-posta elettronika għal dan il-għan ġie skoraġġut. Il-passwords maħżuna fil-bażi ta' *data* ġew hashed b'algoritmu b'saħħtu u l-melħ ma ġiex kompromess. *Data* affettwata: passwords hashed ta' 1 200 utent. Għal raġunijiet ta' sikurezza, il-kontrollur informa lis-suġġetti tad-*data* dwar il-ksur permezz tal-posta elettronika u talabhom ibiddlu l-passwords tagħhom, speċjalment jekk l-istess password intużat għal servizzi oħrajn.

3.2.1 KAŻ Nru 06 - Miżuri preventivi u valutazzjoni tar-riskju

56. F'dan il-każ partikolari, il-kunfidenzjalità tad-*data* hija kompromessa, iżda l-passwords fil-bażi ta' *data* kienu hashed b'metodu aġġornat, li jnaqqas ir-riskju fir-rigward tan-natura, is-sensittività u l-volum ta' *data* personali. Dan il-każ ma jippreżenta l-ebda riskju għad-drittijiet u l-libertajiet tas-suġġetti tad-*data*.

57. Barra minn hekk, ma ġiet kompromessa l-ebda informazzjoni ta' kuntatt (eż. indirizzi tal-posta elettronika jew numri tat-telefon) tas-suġġetti tad-*data*, li jfisser li ma hemm l-ebda riskju sinifikanti għas-suġġetti tad-*data* li jkunu fil-mira ta' tentattivi ta' frodi (eż. li jirċievu posta elettronika ta' phishing jew messaġġi u telefonati frawdolenti). Ma kienet involuta l-ebda kategorija speċjali ta' *data* personali.

58. Xi identifikaturi tal-utent jistgħu jitqiesu bħala *data* personali, iżda s-suġġett tas-sit web ma jippermettix konnotazzjonijiet negattivi. Għalkemm għandu jiġi nnotat li l-valutazzjoni tar-riskju tista' tinbidel[20] jekk it-tip tas-sit web u d-*data* aċċessata jistgħu jiżvelaw kategoriji speċjali ta' *data* personali (eż. sit web ta' partit politiku jew ta' trade union). L-użu ta' kriptaġġ tal-ogħla livell ta' żvilupp tekniku jista' jimmitiga l-effetti negattivi tal-ksur. L-iżgurar li jkun permess numru limitat ta' tentattivi ta' lloggjar jipprevjeni attakki ta' lloggjar b'forza brutali milli jirnexxu, u b'hekk jitnaqqsu fil-biċċa l-kbira tar-riskji imposti mill-attakkanti li jkunu diġà jafu l-identifikaturi tal-utenti.

3.2.2 KAŻ Nru 06 – Mitigazzjoni u obbligi

59. Il-komunikazzjoni lis-suġġetti tad-*data* f'xi każijiet tista' titqies bħala fattur ta' mitigazzjoni, peress li s-suġġetti tad-*data* huma wkoll f'pożizzjoni li jieħdu l-passi meħtieġa sabiex jevitaw aktar ħsara minħabba l-ksur, pereżempju billi jibdlu l-password tagħhom. F'dan il-każ, in-notifika ma kinitx obbligatorja, iżda f'ħafna każijiet tista' titqies bħala prattika tajba.

60. Il-kontrollur tad-*data* għandu jikkoreġi l-vulnerabbiltà u jimplimenta miżuri ġodda ta' sigurtà sabiex jiġi evitat ksur simili tad-*data* fil-futur bħal, pereżempju, awditi sistematiċi tas-sigurtà fuq is-sit web.

61. Il-ksur għandu jiġi ddokumentat f'konformità mal-Artikolu 33(5) iżda ma hija meħtieġa l-ebda notifika jew komunikazzjoni.

62. Barra minn hekk, huwa ferm rakkomandat li jiġi kkomunikat ksur li jinvolvi passwords lis-suġġetti tad-*data* fi kwalunkwe każ anke meta l-passwords ikunu nħażnu bl-użu ta' salted hash b'algoritmu li jikkonforma mal-ogħla livell ta' żvilupp tekniku. L-użu ta' metodi ta' awtentikazzjoni li jevitaw il-ħtieġa li jiġu pproċessati passwords min-naħa tas-server huwa preferibbli. Is-suġġetti tad-*data* għandhom jingħataw l-għażla li jieħdu miżuri xierqa fir-rigward tal-passwords tagħhom stess.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati

[20] Għal gwida dwar operazzjonijiet ta' pproċessar li "*x'aktarx jirriżultaw f'riskju għoli*", ara n-nota 10 f'qiegħ il-paġna hawn fuq.

Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	X	X

3.3 KAŻ Nru 07: Attakk ta' ġbir tal-kredenzjali fuq sit web bankarju

Bank ġarrab attakk ċibernetiku kontra wieħed mis-siti web tiegħu ta' servizzi bankarji online. L-attakk kellu l-għan li jelenka l-identifikaturi tal-utent għall-illoggjar kollha possibbli bl-użu ta' password trivjali fissa. Il-passwords jikkonsistu fi 8 ċifri. Minħabba vulnerabbiltà tas-sit web, f'xi każijiet, l-informazzjoni dwar is-suġġetti tad-*data* (l-isem, il-kunjom, il-ġeneru, id-data u l-post tat-twelid, il-kodiċi fiskali, il-kodiċijiet ta' identifikazzjoni tal-utent) ġiet żvelata lill-attakkant, anke jekk il-password użata ma kinitx korretta jew il-kont bankarju ma kienx għadu attiv. Dan affettwa madwar 100 000 suġġett tad-*data*. Minn dawn, l-attakkant illoggja b'suċċess f'madwar 2 000 kont li kienu qegħdin jużaw il-password trivjali pprovata mill-attakkant. Sussegwentement, il-kontrollur seta' jidentifika t-tentattivi illeġittimi ta' log-on kollha. Il-kontrollur tad-*data* seta' jikkonferma li, skont il-kontrolli kontra l-frodi, ma saret l-ebda tranżazzjoni minn dawn il-kontijiet matul l-attakk. Il-bank kien konxju tal-ksur tad-*data* minħabba li ċ-ċentru tal-operazzjonijiet tas-sigurtà tiegħu sab numru kbir ta' talbiet għal illoggjar diretti fis-sit web. B'reazzjoni għal dan, il-kontrollur iddiżattiva l-possibbiltà ta' lloggjar fis-sit web billi tfiha u impona ssettjar ta' password ġdida għall-kontijiet kompromessi. Il-kontrollur ikkomunika l-ksur biss lill-utenti bil-kontijiet kompromessi, jiġifieri lill-utenti li l-passwords tagħhom ġew kompromessi jew li d-*data* tagħhom ġiet żvelata.

3.3.1 KAŻ Nru 07 - Miżuri preventivi u valutazzjoni tar-riskju

63. Huwa importanti li jingħad li l-kontrolluri li jittrattaw *data* ta' natura personali ħafna[21] għandhom responsabbiltà akbar f'termini ta' forniment ta' sigurtà tad-*data* adegwata, eż. li jkollhom ċentru tal-operazzjonijiet tas-sigurtà u miżuri oħrajn ta' prevenzjoni, detezzjoni u rispons għall-inċidenti. In-nuqqas ta' konformità ma' dawn l-istandards ogħla ċertament jirriżulta f'miżuri aktar serji matul investigazzjoni tal-SA.

64. Il-ksur jikkonċerna *data* finanzjarja lil hinn mill-identità u l-informazzjoni dwar l-identifikatur tal-utent, u dan jagħmlu partikolarment sever. In-numru ta' individwi affettwati huwa għoli.

65. Il-fatt li ksur jista' jseħħ f'ambjent sensittiv bħal dan jindika nuqqasijiet sinifikanti ta' sigurtà tad-*data* fis-sistema tal-kontrollur, u jista' jkun indikatur li huwa żmien li fih huma "meħtieġa" rieżami u aġġornament tal-miżuri affettwati f'konformità mal-Artikoli 24(1), 25(1), u 32(1) tal-GDPR. Id-*data* li fuqha tkun seħħet vjolazzjoni tippermetti l-identifikazzjoni unika tas-suġġetti tad-*data* u fiha informazzjoni oħra dwarhom (inklużi l-ġeneru, id-data u l-post tat-twelid), barra minn hekk tista' tintuża mill-attakkant sabiex jaqta' l-passwords tal-klijenti jew sabiex imexxi kampanja ta' phishing immirata lejn il-klijenti tal-bank.

66. Għal dawn ir-raġunijiet, il-ksur tad-*data* tqies li x'aktarx jirriżulta f'riskju għoli għad-drittijiet u l-libertajiet tas-suġġetti kollha tad-*data* kkonċernati[22]. Għalhekk, l-okkorrenza ta' ħsara materjali (eż. telf finanzjarju) u mhux materjali (eż. serq tal-identità jew frodi) hija riżultat konċepibbli.

---

[21] Bħall-informazzjoni tas-suġġetti tad-*data* msemmija fil-metodi ta' ħlas bħal numri tal-kards, kontijiet bankarji, ħlas online, pagi, dikjarazzjonijiet bankarji, studji ekonomiċi jew kwalunkwe informazzjoni oħra li tista' tiżvela informazzjoni ekonomika relatata mas-suġġetti tad-*data*.

[22] Għal gwida dwar operazzjonijiet ta' pproċessar li "*x'aktarx jirriżultaw f'riskju għoli*", ara n-nota 10 f'qiegħ il-paġna hawn fuq.

3.3.2 KAŻ Nru 07 – Mitigazzjoni u obbligi

67. Il-miżuri tal-kontrollur imsemmija fid-deskrizzjoni tal-każ huma adegwati. Fid-dawl tal-ksur, huwa kkoreġa wkoll il-vulnerabbiltà tas-sit web u ħa passi oħrajn sabiex jipprevjeni ksur simili tad-*data* fil-futur, bħaż-żieda ta' awtentikazzjoni b'żewġ fatturi għas-sit web ikkonċernat u t-tranżizzjoni lejn awtentikazzjoni qawwija tal-konsumatur.

68. Id-dokumentazzjoni tal-ksur skont l-Artikolu 33(5) tal-GDPR u n-notifika lill-SA dwaru ma humiex fakultattivi f'dan ix-xenarju. Barra minn hekk, il-kontrollur għandu jinnotifika l-100 000 suġġett tad-*data* kollha (inklużi s-suġġetti tad-*data* li l-kontijiet tagħhom ma kinux kompromessi) f'konformità mal-Artikolu 34 tal-GDPR.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	✓	✓

3.4 Miżuri organizzazzjonali u tekniċi għall-prevenzjoni/għall-mitigazzjoni tal-impatti tal-attakki minn hackers

69. Bħal fil-każ ta' attakki ransomware, irrispettivament mir-riżultat u mill-konsegwenzi tal-attakk, l-evalwazzjoni mill-ġdid tas-sigurtà tal-IT hija obbligatorja għall-kontrolluri f'każijiet simili.

70. Miżuri rakkomandati:[23]

(*Il-lista tal-miżuri li ġejjin bl-ebda mod ma hija esklużiva jew komprensiva. Pjuttost, l-għan huwa li jiġu pprovduti ideat għall-prevenzjoni u soluzzjonijiet possibbli. Kull attività ta' proċessar hija differenti, għalhekk il-kontrollur għandu jieħu d-deċiżjoni dwar liema miżuri huma l-aktar adatti għas-sitwazzjoni partikolari.*)

- Kriptaġġ tal-ogħla livell ta' żvilupp tekniku u mmaniġġar essenzjali, speċjalment meta jkunu qegħdin jiġu pproċessati passwords u *data* sensittiva jew finanzjarja. Il-hashing kriptografiku u s-salting għal informazzjoni sigrieta (passwords) dejjem huma ppreferuti mill-kriptaġġ tal-passwords. L-użu ta' metodi ta' awtentikazzjoni li jevitaw il-ħtieġa li jiġu pproċessati passwords min-naħa tas-server huwa preferibbli.
- L-aġġornament tas-sistema (software u firmware). L-iżgurar li jkunu stabbiliti l-miżuri kollha ta' sigurtà tal-IT, filwaqt li jiġi żgurat li dawn ikunu effettivi u li jinżammu aġġornati b'mod regolari meta jinbidlu jew jevolvu l-ipproċessar jew iċ-ċirkostanzi. Sabiex ikun jista' juri l-konformità mal-Artikolu 5(1)(f) f'konformità mal-Artikolu 5(2) tal-GDPR, il-kontrollur għandu jżomm rekord tal-aġġornamenti kollha mwettqa, inkluż ukoll iż-żmien meta ġew applikati.
- L-użu ta' metodi ta' awtentikazzjoni b'saħħithom bħal awtentikazzjoni b'żewġ fatturi u servers tal-awtentikazzjoni, ikkomplementati minn politika aġġornata dwar il-passwords.
- Standards ta' żvilupp siguri jinkludu l-filtrazzjoni tal-input tal-utent (bl-użu ta' lista bajda sa fejn ikun prattikabbli), il-ħrib minn inputs tal-utent u miżuri ta' prevenzjoni b'forza brutali (bħal-limitazzjoni tal-ammont massimu ta' provi mill-ġdid). "Firewalls għall-Applikazzjonijiet tal-Web" jistgħu jgħinu fl-użu effettiv ta' din it-teknika.
- L-istabbiliment ta' privileġġi tal-utent b'saħħithom u politika dwar l-immaniġġar tal-kontroll tal-aċċess.
- L-użu ta' sistemi xierqa, aġġornati, effettivi u integrati tal-firewall, ta' detezzjoni tal-intrużjonijiet u ta' sistemi oħrajn ta' difiża tal-perimetru.
- Awditi sistematiċi tas-sigurtà tal-IT u valutazzjonijiet tal-vulnerabbiltà (ittestjar tal-penetrazzjoni).

[23] Għall-iżvilupp sigur tal-applikazzjonijiet tal-web ara wkoll: https://www.owasp.org/index.php/Main_Page .

- Rieżamijiet u ttestjar regolari sabiex jiġi żgurat li l-kopji ta' riżerva jkunu jistgħu jintużaw sabiex tiġi rrestawrata kwalunkwe *data* li l-integrità jew id-disponibbiltà tagħha tkun ġiet affettwata.
- L-ebda identifikazzjoni tas-sessjoni fil-URL f'format ta' test sempliċi.

4 SORS INTERN TA' RISKJU UMAN

71. Ir-rwol tal-iżball uman fil-ksur ta' *data* personali għandu jiġi enfasizzat, minħabba d-dehra komuni tiegħu. Peress li dawn it-tipi ta' ksur jistgħu jkunu kemm intenzjonati kif ukoll mhux intenzjonati, huwa diffiċli ħafna għall-kontrolluri tad-*data* li jidentifikaw il-vulnerabbiltajiet u jadottaw miżuri sabiex jevitawhom. Il-Konferenza Internazzjonali tal-Kummissarji għall-Protezzjoni tad-*Data* u l-Privatezza rrikonoxxiet l-importanza li jiġu indirizzati tali fatturi umani u adottat ir-riżoluzzjoni sabiex jiġi indirizzat ir-rwol tal-iżball uman fil-ksur tad-*data* personali f'Ottubru tal-2019[24]. Din ir-riżoluzzjoni tisħaq li għandhom jittieħdu miżuri xierqa ta' salvagwardja sabiex jiġu evitati l-iżbalji umani u tipprovdi lista mhux eżawrjenti ta' tali salvagwardji u approċċi.

4.1 KAŻ Nru 08: Eksfiltrazzjoni ta' *data* tan-negozju minn impjegat

Matul il-perjodu ta' avviż tiegħu, l-impjegat ta' kumpanija kkopja *data* tan-negozju mill-bażi ta' *data* tal-kumpanija. L-impjegat huwa biss awtorizzat li jaċċessa d-*data* sabiex iwettaq il-kompiti ta' impjieg tiegħu. Xhur wara, wara li waqaf mix-xogħol, huwa uża d-*data* miksuba b'dan il-mod (*data* ta' kuntatt bażika) sabiex jikkontribwixxi għall-ipproċessar tad-*data* ġdid li għalih huwa l-kontrollur sabiex jikkuntattja lill-klijenti tal-kumpanija sabiex iħajjarhom għan-negozju l-ġdid tiegħu.

4.1.1 KAŻ Nru 08 - Miżuri preventivi u valutazzjoni tar-riskju

72. F'dan il-każ partikolari ma ttieħdet l-ebda miżura preventiva sabiex l-impjegat ma jitħalliex jikkopja informazzjoni ta' kuntatt ta' klijenti tal-kumpanija, peress li kien jeħtieġ – u kellu – aċċess leġittimu għal din l-informazzjoni minħabba l-kompiti ta' impjieg tiegħu. Peress li l-issodisfar tal-biċċa l-kbira tal-impjiegi relatati mal-klijenti jirrikjedi xi tip ta' aċċess għal *data* personali mill-impjegati, jista' jkun aktar diffiċli li jiġi pprevenut dan il-ksur tad-*data*. Il-limitazzjonijiet għall-ambitu tal-aċċess jistgħu jillimitaw ix-xogħol li jkun jista' jagħmel l-impjegat partikolari. Madankollu, politiki ta' aċċess maħsuba sew u kontroll kostanti jistgħu jgħinu fil-prevenzjoni ta' tali ksur.

73. Bħas-soltu, matul il-valutazzjoni tar-riskju, għandhom jitqiesu t-tip ta' ksur u n-natura, is-sensittività u l-volum tad-*data* personali affettwata. Dawn it-tipi ta' ksur huma tipikament ksur tal-kunfidenzjalità, peress li l-bażi ta' *data* normalment titħalla intatta, u l-kontenut tagħha "sempliċiment" jiġi kkopjat għal użu ulterjuri. Il-kwantità ta' *data* affettwata normalment tkun ukoll baxxa jew medja. F'dan il-każ partikolari ma ġiet affettwata l-ebda kategorija speċjali ta' *data* personali, l-impjegat kellu bżonn biss l-informazzjoni ta' kuntatt tal-klijenti sabiex ikun jista' jikkuntattjahom wara li jkun telaq mill-kumpanija. Għalhekk, id-*data* kkonċernata ma hijiex sensittiva.

74. Għalkemm l-uniku għan tal-eks impjegat li kkopja d-*data* b'mod malizzjuż għandu mnejn ikun limitat għall-ksib ta' informazzjoni ta' kuntatt tal-klijenti tal-kumpanija għall-finijiet kummerċjali tiegħu stess, il-kontrollur

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf

ma huwiex f'pożizzjoni li jqis li r-riskju għas-suġġetti tad-*data* affettwati jkun baxx, peress li l-kontrollur ma għandu l-ebda tip ta' riassigurazzjoni dwar l-intenzjonijiet tal-impjegat. Għalhekk, filwaqt li l-konsegwenzi tal-ksur jistgħu jkunu limitati għal esponiment għal awtopromozzjoni mhux mitlub mill-eks impjegat, ma jiġix eskluż abbuż ulterjuri u aktar gravi tad-*data* misruqa, skont l-iskop tal-ipproċessar stabbilit mill-eks impjegat[25].

4.1.2 KAŻ Nru 08 – Mitigazzjoni u obbligi

75. Il-mitigazzjoni tal-effetti negattivi tal-ksur fil-każ ta' hawn fuq hija diffiċli. Jista' jkun meħtieġ li tiġi involuta azzjoni legali immedjata sabiex tipprevjeni lill-eks impjegat milli jabbuża mid-*data* u jxerridha aktar. Bħala l-pass li jmiss, l-għan għandu jkun li jiġu evitati sitwazzjonijiet futuri simili. Il-kontrollur jista' jipprova jordna lill-eks impjegat jieqaf juża d-*data*, iżda hemm dubji kbar kemm din l-azzjoni jkollha suċċess. Miżuri tekniċi xierqa bħall-impossibbiltà li tiġi kkopjata jew li titniżżel id-*data* fuq apparat li jista' jitneħħa jistgħu jgħinu.

76. Ma hemm l-ebda soluzzjoni universali għal dawn it-tipi ta' każijiet, iżda approċċ sistematiku jista' jgħin fil-prevenzjoni tagħhom. Pereżempju, il-kumpanija tista' tikkunsidra – meta jkun possibbli – li tirtira ċerti forom ta' aċċess għal impjegati li jkunu wrew l-intenzjoni tagħhom li jieqfu jew li jimplimentaw log fajls ta' aċċess sabiex l-aċċess mhux mixtieq ikun jista' jiġi lloggjat u indikat. Il-kuntratt iffirmat mal-impjegati għandu jinkludi klawżoli li jipprojbixxu tali azzjonijiet.

77. Fl-aħħar mill-aħħar, peress li dan il-ksur partikolari ma huwiex se jirriżulta f'riskju għoli għad-drittijiet u l-libertajiet tal-persuni fiżiċi, notifika lill-SA tkun biżżejjed. Madankollu, l-għoti ta' informazzjoni lis-suġġetti tad-*data* jista' jkun ta' benefiċċju għall-kontrollur tad-*data* wkoll, peress li jista' jkun aħjar li jisimgħu mingħand il-kumpanija dwar l-iżvelar tad-*data* milli mingħand l-eks impjegat li jipprova jikkuntattjahom. Id-dokumentazzjoni dwar il-ksur tad-*data* f'konformità mal-Artikolu 33(5) hija obbligu legali.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	✓	X

[25] Għal gwida dwar operazzjonijiet ta' pproċessar li "*x'aktarx jirriżultaw f'riskju għoli*", ara n-nota 10 f'qiegħ il-paġna hawn fuq.

4.2 KAŻ Nru 09: Trażmissjoni aċċidentali ta' *data* lil parti terza fdata

Aġent tal-assigurazzjoni nnota li – permezz tas-settings difettużi ta' fajl Excel riċevut bil-posta elettronika – huwa seta' jaċċessa informazzjoni relatata ma' 24 klijent li ma jaqgħux taħt il-qasam tiegħu. Huwa marbut bis-segretezza professjonali u kien l-uniku riċevitur ta' din il-posta elettronika. L-arranġament bejn il-kontrollur tad-*data* u l-aġent tal-assigurazzjoni jobbliga lill-aġent jindika ksur ta' *data* personali mingħajr dewmien żejjed lill-kontrollur tad-*data*. Għalhekk, l-aġent mill-ewwel indika l-iżball lill-kontrollur, li kkoreġa l-fajl u reġa' bagħtu, filwaqt li talab lill-aġent iħassar il-messaġġ preċedenti. Skont l-arranġament imsemmi hawn fuq, l-aġent irid jikkonferma t-tħassir f'dikjarazzjoni bil-miktub, u dan għamlu. L-informazzjoni miksuba ma tinkludi l-ebda kategorija speċjali ta' *data* personali, iżda *data* ta' kuntatt u *data* dwar l-assigurazzjoni nnifisha (tip ta' assigurazzjoni, ammont) biss. Wara li analizza d-*data* personali affettwata mill-ksur, il-kontrollur tad-*data* ma identifika l-ebda karatteristika speċjali fuq in-naħa tal-individwi jew tal-kontrollur tad-*data* li tista' taffettwa l-livell ta' impatt tal-ksur.

4.2.1 KAŻ Nru 09 – Miżuri preventivi u valutazzjoni tar-riskju

78. F'dan il-każ, il-ksur ma jirriżultax minn azzjoni intenzjonata ta' impjegat, iżda minn żball uman mhux intenzjonat ikkawżat minn nuqqas ta' attenzjoni. Dawn it-tipi ta' ksur jistgħu jiġu evitati jew imnaqqsa fil-frekwenza permezz ta' a) l-infurzar ta' programmi ta' taħriġ, edukazzjoni u sensibilizzazzjoni fejn l-impjegati jiksbu fehim aħjar tal-importanza tal-protezzjoni tad-*data* personali, b) it-tnaqqis tal-iskambju tal-fajls permezz tal-posta elettronika, u l-użu, minflok, ta' sistemi ddedikati għall-ipproċessar tad-*data* tal-klijenti pereżempju, c) il-verifika doppja tal-fajls qabel jintbagħtu, d) is-separazzjoni tal-ħolqien u t-trażmissjoni tal-fajls.

79. Dan il-ksur tad-*data* jikkonċerna biss il-kunfidenzjalità tad-*data*, u l-integrità u l-aċċessibbiltà tagħha jitħallew intatti. Il-ksur tad-*data* kien jikkonċerna biss madwar 24 klijent, u għalhekk il-kwantità tad-*data* affettwata tista' titqies bħala baxxa. Barra minn hekk, id-*data* personali affettwata ma fiha l-ebda *data* sensittiva. Il-fatt li l-proċessur tad-*data* ikkuntattja minnufih lill-kontrollur tad-*data* wara li sar konxju tal-ksur tad-*data* jista' jitqies bħala fattur ta' mitigazzjoni tar-riskju. (Il-possibbiltà li d-*data* tkun intbagħtet lil aġenti oħrajn tal-assigurazzjoni għandha tiġi evalwata wkoll u, jekk tiġi kkonfermata, għandhom jittieħdu miżuri xierqa.) Minħabba l-passi xierqa meħuda wara l-ksur tad-*data*, dan probabbilment ma huwa se jkollu l-ebda impatt fuq id-drittijiet u l-libertajiet tas-suġġetti tad-*data*.

80. Il-kombinament tan-numru baxx ta' individwi affettwati, is-sejba immedjata tal-ksur u l-miżuri meħuda sabiex dawn l-effetti jiġu mminimizzati jagħmlu dan il-każ partikolari wieħed mingħajr riskju.

4.2.2 KAŻ Nru 09 – Mitigazzjoni u obbligi

81. Barra minn hekk, hemm ċirkostanzi oħrajn ta' mitigazzjoni tar-riskju involuti wkoll: l-aġent ikun marbut bis-segretezza professjonali; huwa stess irrapporta l-problema lill-kontrollur; u huwa ħassar il-fajl fuq talba. Is-sensibilizzazzjoni u, possibbilment, l-inklużjoni ta' passi addizzjonali fil-verifika tad-dokumenti li jinvolvu *data* personali probabbilment se jgħinu sabiex jiġu evitati każijiet simili fil-futur.

82. Minbarra d-dokumentazzjoni tal-ksur f'konformità mal-Artikolu 33(5), ma hemm ebda ħtieġa għal azzjoni oħra.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	X	X

4.3 Miżuri organizzazzjonali u tekniċi għall-prevenzjoni/għall-mitigazzjoni tal-impatti ta' sorsi interni ta' riskju uman

83. Kombinament tal-miżuri msemmija hawn taħt – applikati skont il-karatteristiċi uniċi tal-każ – għandu jgħin sabiex jitnaqqas iċ-ċans li jerġa' jseħħ ksur simili.

84. Miżuri rakkomandati:

(*Il-lista tal-miżuri li ġejjin bl-ebda mod ma hija esklużiva jew komprensiva. Pjuttost, l-għan huwa li jiġu pprovduti ideat għall-prevenzjoni u soluzzjonijiet possibbli. Kull attività ta' pproċessar hija differenti, għalhekk il-kontrollur għandu jieħu d-deċiżjoni dwar liema miżuri huma l-aktar adatti għas-sitwazzjoni partikolari.*)

- L-implimentazzjoni perjodika ta' programmi ta' taħriġ, edukazzjoni u sensibilizzazzjoni għall-impjegati dwar l-obbligi tagħhom ta' privatezza u sigurtà u d-detezzjoni u r-rapportar ta' theddid għas-sigurtà tad-*data* personali[26]. L-iżvilupp ta' programm ta' sensibilizzazzjoni sabiex ifakkar lill-impjegati fl-aktar żbalji komuni li jwasslu għal ksur ta' *data* personali u kif għandhom jiġu evitati.
- L-istabbiliment ta' prattiki, proċeduri u sistemi robusti u effettivi għall-protezzjoni tad-*data* u l-privatezza[27].
- Evalwazzjoni tal-prattiki, tal-proċeduri u tas-sistemi ta' privatezza sabiex tiġi żgurata effettività kontinwa[28].
- It-twettiq ta' politiki xierqa ta' kontroll tal-aċċess u li l-utenti jiġu mġiegħla jsegwu r-regoli.
- Tekniki ta' implimentazzjoni sabiex l-awtentikazzjoni tal-utent tiġi infurzata meta tiġi aċċessata *data* personali sensittiva.
- Id-diżattivazzjoni tal-kont tal-utent relatat mal-kumpanija hekk kif il-persuna tħalli l-kumpanija.
- Il-verifika ta' flussi ta' *data* mhux tas-soltu bejn is-server tal-fajls u l-istazzjonijiet tax-xogħol tal-impjegati.
- L-istabbiliment ta' sigurtà tal-interfaċċa I/O fil-BIOS jew permezz tal-użu ta' software li jikkontrolla l-użu ta' interfaċċi tal-kompjuter (l-illukkjar jew il-ftuħ ta' pereżempju USB/CD/DVD eċċ.).
- Rieżaminar tal-politika ta' aċċess tal-impjegati (eż. l-illoggjar ta' aċċess għal *data* sensittiva u l-infurzar tal-ħtieġa li l-utent jagħti raġuni professjonali, sabiex din tkun disponibbli għall-awditi).
- Id-diżattivazzjoni tas-servizzi tal-cloud miftuħa.
- Il-projbizzjoni u l-prevenzjoni tal-aċċess għal servizzi tal-posta miftuħa magħrufa.
- Id-diżattivazzjoni tal-funzjoni ta' print screen fl-OS.
- L-infurzar ta' politika ta' skrivanija nadifa.
- L-imblukkar awtomatiku tal-kompjuters kollha wara ċertu ammont ta' ħin ta' inattività.
- L-użu ta' mekkaniżmi (eż. token (mingħajr fili) sabiex jiġu aċċessati/jinfetħu kontijiet imsakkrin) għal qlib rapidu tal-utenti f'ambjenti kondiviżi.
- L-użu ta' sistemi ddedikati għall-immaniġġar tad-*data* personali li japplikaw mekkaniżmi xierqa ta' kontroll tal-aċċess u li jipprevjenu l-iżball uman, bħall-bgħit ta' komunikazzjonijiet lis-suġġett żbaljat. L-użu ta' spreadsheets u ta' dokumenti oħrajn tal-uffiċċju ma huwiex mezz xieraq għall-immaniġġar tad-*data* tal-klijenti.

[26] Is-sottotaqsima (i) tat-Taqsima 2) tar-Riżoluzzjoni sabiex jiġi indirizzat ir-rwol ta' żball uman fi ksur ta' *data* personali.

[27] Is-sottotaqsima (ii) tat-Taqsima 2) tar-Riżoluzzjoni sabiex jiġi indirizzat ir-rwol ta' żball uman fi ksur ta' *data* personali.

[28] Is-sottotaqsima (iii) tat-Taqsima 2) tar-Riżoluzzjoni sabiex jiġi indirizzat ir-rwol ta' żball uman fi ksur ta' *data* personali.

5 APPARAT U DOKUMENTI STAMPATI MITLUFA JEW MISRUQA

85. Tip ta' każ frekwenti huwa t-telf jew is-serq ta' apparat portabbli. F'dawn il-każijiet, il-kontrollur irid iqis iċ-ċirkostanzi tal-operazzjoni ta' pproċessar, bħat-tip ta' *data* maħżuna fuq l-apparat, kif ukoll l-assi ta' sostenn, u l-miżuri meħuda qabel il-ksur sabiex jiġi żgurat livell xieraq ta' sigurtà. Dawn l-elementi kollha jaffettwaw l-impatti potenzjali tal-ksur tad-*data*. Il-valutazzjoni tar-riskju tista' tkun diffiċli, peress li l-apparat ma jkunx għadu disponibbli.

86. Dawn it-tipi ta' ksur dejjem jistgħu jiġu kklassifikati bħala ksur tal-kunfidenzjalità. Madankollu, jekk ma jkun hemm l-ebda kopja ta' riżerva tal-bażi ta' *data* misruqa, it-tip ta' ksur jista' jkun ukoll ksur ta' disponibbiltà u ksur ta' integrità.

87. Ix-xenarji li ġejjin juru kif iċ-ċirkostanzi msemmija hawn fuq jinfluwenzaw il-probabbiltà u s-severità tal-ksur tad-*data*.

5.1 KAŻ Nru 10: Materjal misruq li fih hemm maħżuna *data* personali kriptata

Waqt serqa minn ċentru għall-kura ta' matul il-jum tat-tfal, insterqu żewġ tablets. It-tablets kien fihom applikazzjoni li kellha *data* personali dwar it-tfal li jattendu ċ-ċentru għall-kura ta' matul il-jum. L-isem, id-data tat-twelid u d-*data* personali dwar l-edukazzjoni tat-tfal kienu involuti. Kemm it-tablets kriptati, li kienu mitfija fil-ħin tas-serqa, kif ukoll l-applikazzjoni kienu protetti permezz ta' password b'saħħitha. Il-kopja ta' riżerva tad-*data* kienet disponibbli b'mod effettiv u faċli għall-kontrollur. Wara li sar konxju mill-ksur, iċ-ċentru għall-kura ta' matul il-jum ħassar id-*data* maħżuna fuq it-tablets mill-bogħod ftit wara li saret magħrufa s-serqa.

5.1.1 KAŻ Nru 10 - Miżuri preventivi u valutazzjoni tar-riskju

88. F'dan il-każ partikolari, il-kontrollur tad-*data* ħa miżuri adegwati sabiex jipprevjeni u jimmitiga l-impatti ta' ksur potenzjali tad-*data* bl-użu ta' kriptaġġ tal-apparat, bl-introduzzjoni ta' protezzjoni adegwata permezz ta' password u bl-iżgurar ta' kopja ta' riżerva tad-*data* maħżuna fit-tablets. (Lista ta' miżuri rakkomandati tinsab fit-Taqsima 5.7).

89. Wara li jsir konxju ta' ksur, il-kontrollur tad-*data* għandu jivvaluta s-sors tar-riskju, is-sistemi li jappoġġaw l-ipproċessar tad-*data*, it-tip ta' *data* personali involuta u l-impatti potenzjali tal-ksur tad-*data* fuq l-individwi kkonċernati. Il-ksur tad-*data* deskritt hawn fuq kien jikkonċerna l-kunfidenzjalità, id-disponibbiltà u l-integrità tad-*data* kkonċernata, madankollu minħabba l-proċedimenti xierqa tal-kontrollur tad-*data* qabel u wara l-ksur tad-*data*, l-ebda waħda minn dawn ma seħħet.

5.1.2 KAŻ Nru 10 – Mitigazzjoni u obbligi

90. Il-kunfidenzjalità tad-*data* personali fit-tablets ma ġietx kompromessa minħabba l-protezzjoni qawwija tal-password kemm tat-tablet kif ukoll tal-applikazzjonijiet. It-tablets ġew issettjati b'tali mod li l-issettjar ta' password ifisser ukoll li d-*data* maħżuna fuq l-apparat tkun kriptata. Dan kompla jissaħħaħ bl-azzjoni tal-kontrollur sabiex jipprova jħassar kollox minn fuq l-apparat misruq mill-bogħod.

91. Minħabba l-miżuri meħuda, il-kunfidenzjalità tad-*data* nżammet intatta wkoll. Barra minn hekk, il-kopja ta' riżerva żgurat id-disponibbiltà kontinwa tad-*data* personali, u b'hekk ma seta' jseħħ l-ebda impatt negattiv potenzjali.

92. Minħabba dawn il-fatti, il-ksur tad-*data* deskritt hawn fuq x'aktarx li ma jirriżultax f'riskju għad-drittijiet u l-libertajiet tas-suġġetti tad-*data*, u b'hekk ma kienet meħtieġa l-ebda notifika lill-SA jew lis-suġġetti tad-*data* kkonċernati. Madankollu, dan il-ksur tad-*data* jrid jiġi ddokumentat ukoll f'konformità mal-Artikolu 33(5).

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	X	X

5.2 KAŻ Nru 11: Materjal misruq li fih hemm maħżuna *data* personali mhux kriptata

Insteraq notebook elettroniku ta' impjegat ta' kumpanija li tipprovdi s-servizzi. In-notebook misruq kien fih l-ismijiet, il-kunjomijiet, is-sess, l-indirizzi u d-data tat-twelid ta' aktar minn 100 000 klijent. Minħabba n-nuqqas ta' disponibbiltà tal-apparat misruq ma kienx possibbli li jiġi identifikat jekk kategoriji oħrajn ta' *data* personali kinux affettwati wkoll. L-aċċess għall-hard drive tan-notebook ma kien protett bl-ebda password. Id-*data* personali tista' tiġi rrestawrata mill-kopja ta' riżerva disponibbli li ssir kuljum.

5.2.1 KAŻ Nru 11 - Miżuri preventivi u valutazzjoni tar-riskju

93. Ma ttieħdet l-ebda miżura ta' sikurezza preventiva mill-kontrollur tad-*data*, u għalhekk id-*data* personali maħżuna fin-notebook misruq kienet faċilment aċċessibbli għall-ħalliel jew għal kwalunkwe persuna oħra li tikseb pussess tal-apparat fil-futur.

94. Dan il-ksur ta' *data* jikkonċerna l-kunfidenzjalità tad-*data* maħżuna fuq l-apparat misruq.

95. In-notebook li fih id-*data* personali kien vulnerabbli f'dan il-każ minħabba li ma kien protett bl-ebda password jew kriptaġġ. In-nuqqas ta' miżuri bażiċi ta' sigurtà jżid il-livell ta' riskju għas-suġġetti tad-*data* affettwati. Barra minn hekk, l-identifikazzjoni tas-suġġetti tad-*data* kkonċernati hija wkoll problematika, u dan iżid ukoll is-severità tal-ksur. In-numru konsiderevoli ta' individwi kkonċernati jżid ir-riskju, madankollu, l-ebda kategorija speċjali ta' *data* personali ma kienet ikkonċernata fil-ksur tad-*data*.

96. Matul il-valutazzjoni tar-riskju[29], il-kontrollur għandu jqis il-konsegwenzi potenzjali u l-effetti negattivi tal-ksur tal-kunfidenzjalità. Bħala riżultat tal-ksur, is-suġġetti tad-*data* kkonċernati jistgħu jġarrbu frodi tal-identità tagħhom li jiddependi fuq id-*data* disponibbli fuq l-apparat misruq, u għalhekk ir-riskju jitqies bħala għoli.

5.2.2 KAŻ Nru 11 – Mitigazzjoni u obbligi

97. Il-kriptaġġ tal-apparat operattiv u l-użu ta' protezzjoni permezz ta' password qawwija għall-bażi ta' *data* maħżuna setgħu jipprevjenu l-ksur tad-*data* milli jirriżulta f'riskju għoli għad-drittijiet u l-libertajiet tas-suġġetti tad-*data*.

[29] Għal gwida dwar operazzjonijiet ta' pproċessar li "*x'aktarx jirriżultaw f'riskju għoli*", ara n-nota 10 f'qiegħ il-paġna hawn fuq.

98. Minħabba dawn iċ-ċirkostanzi, hija meħtieġa notifika lill-SA, filwaqt li hija meħtieġa wkoll notifika lis-suġġetti tad-*data* kkonċernati.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	✓	✓

5.3 KAŻ Nru 12: Fajls f'format stampat b'*data* sensittiva misruqa

Reġistru f'format stampat insteraq minn faċilità ta' riabilitazzjoni mill-vizzju tad-droga. Il-ktieb kien fih *data* bażika dwar l-identità u s-saħħa tal-pazjenti ammessi fil-faċilità ta' riabilitazzjoni. Id-*data* kienet maħżuna biss f'format stampat u ma kien hemm l-ebda kopja ta' riżerva disponibbli għat-tobba li kienu qegħdin jittrattaw il-pazjenti. Il-ktieb ma kienx maħżun f'kexxun jew f'kamra msakkra, u l-kontrollur tad-*data* la kellu sistema ta' kontroll tal-aċċess u lanqas xi miżura oħra ta' salvagwardja għad-dokumentazzjoni f'format stampat.

5.3.1 KAŻ Nru 12 – Miżuri preventivi u valutazzjoni tar-riskju

99. Ma ttieħdet l-ebda miżura ta' sikurezza preventiva mill-kontrollur tad-*data*, u għalhekk id-*data* personali maħżuna f'dan il-ktieb kienet faċilment aċċessibbli għall-persuna li sabitu. Barra minn hekk, in-natura tad-*data* personali maħżuna fil-ktieb tagħmel in-nuqqas ta' kopja ta' riżerva tad-*data* fattur ta' riskju serju ħafna.

100. Dan il-każ iservi bħala eżempju ta' ksur ta' *data* ta' riskju għoli. Minħabba n-nuqqas ta' prekawzjonijiet xierqa għas-sikurezza, intilfet *data* sensittiva dwar is-saħħa skont l-Artikolu 9(1) tal-GDPR. Peress li f'dan il-każ kienet ikkonċernata kategorija speċjali ta' *data* personali, żdiedu r-riskji potenzjali għas-suġġetti tad-*data* kkonċernati, li għandhom jitqiesu wkoll mill-kontrollur li jivvaluta r-riskju[30].

101. Dan il-ksur jikkonċerna l-kunfidenzjalità, id-disponibbiltà u l-integrità tad-*data* personali kkonċernata. Bħala riżultat tal-ksur, is-segretezza medika tinkiser u partijiet terzi mhux awtorizzati jistgħu jiksbu aċċess għall-informazzjoni medika privata tal-pazjenti, li jista' jkollu impatt serju fuq il-ħajja personali tal-pazjent. Il-ksur tad-disponibbiltà jista' jfixkel ukoll il-kontinwità tat-trattament tal-pazjenti. Peress li l-modifika/t-tħassir ta' partijiet mill-kontenut tal-ktieb ma jistgħux jiġu eskluži, l-integrità tad-*data* personali tiġi kompromessa wkoll.

5.3.2 KAŻ Nru 12 – Mitigazzjoni u obbligi

102. Matul il-valutazzjoni tal-miżuri ta' salvagwardja, għandu jitqies ukoll it-tip ta' assi ta' sostenn. Peress li r-reġistru tal-pazjenti kien dokument fiżiku, is-salvagwardja tiegħu kellha tiġi organizzata b'mod differenti minn dik ta' apparat elettroniku. Il-psewdonimizzazzjoni tal-ismijiet tal-pazjenti, il-ħżin tal-ktieb f'bini protett u f'kexxun jew f'kamra msakkra, u l-kontroll xieraq tal-aċċess bl-awtentikazzjoni meta dan jiġi aċċessat setgħu jevitaw il-ksur tad-*data*.

103. Il-ksur tad-*data* deskritt hawn fuq jista' jkollu impatt serju fuq is-suġġetti tad-*data* kkonċernati; għalhekk, in-notifika lill-SA u l-komunikazzjoni tal-ksur lis-suġġetti tad-*data* kkonċernati huma obbligatorji.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	omunikazzjoni lis-suġġetti tad-*data*
✓	✓	✓

[30] Għal gwida dwar operazzjonijiet ta' pproċessar li "*x'aktarx jirriżultaw f'riskju għoli*", ara n-nota 10 f'qiegħ il-paġna hawn fuq.

5.4 Miżuri organizzazzjonali u tekniċi għall-prevenzjoni/għall-mitigazzjoni tal-impatti tat-telf jew tas-serq ta' apparat

104. Kombinament tal-miżuri msemmija hawn taħt – applikati skont il-karatteristiċi uniċi tal-każ – għandu jgħin sabiex jitnaqqas iċ-ċans li jerġa' jseħħ ksur simili.

105. Miżuri rakkomandati:

(*Il-lista tal-miżuri li ġejjin bl-ebda mod ma hija esklużiva jew komprensiva. Pjuttost, l-għan huwa li jiġu pprovduti ideat għall-prevenzjoni u soluzzjonijiet possibbli. Kull attività ta' pproċessar hija differenti, għalhekk il-kontrollur għandu jieħu d-deċiżjoni dwar liema miżuri huma l-aktar adatti għas-sitwazzjoni partikolari.*)

- Il-kriptaġġ tal-apparat operattiv (bħal Bitlocker, Veracrypt jew DM-Crypt).
- L-użu ta' passcode/password fuq l-apparat kollu. Il-kriptaġġ tal-apparat elettroniku mobbli kollu b'mod li jirrikjedi password kumplessa għad-dekriptaġġ.
- L-użu ta' awtentikazzjoni b'diversi fatturi.
- L-attivazzjoni ta' apparat mobbli ħafna operattivi li jippermettulhom jiġu lokalizzati f'każ ta' telf jew ta' tqegħid f'post żbaljat.
- L-użu ta' software/applikazzjoni ta' MDM (Ġestjoni ta' Apparat Mobbli) u l-lokalizzazzjoni. L-użu ta' filtri antiriflessi. L-għeluq ta' kwalunkwe apparat mhux issorveljat.
- Jekk ikun possibbli u xieraq għall-ipproċessar tad-*data* inkwistjoni, l-issejvjar tad-*data* personali fuq back-end server ċentrali, mhux fuq apparat mobbli.
- Jekk l-istazzjon tax-xogħol ikun imqabbad mal-LAN korporattiva, issir kopja ta' riżerva awtomatika mill-folders tax-xogħol sakemm ikun inevitabbli li d-*data* personali tinħażen hemmhekk
- L-użu ta' VPN sigur (eż. li jirrikjedi awtentikazzjoni b'żewġ fatturi sekondarja separata għall-istabbiliment ta' konnessjoni sigura) sabiex l-apparat mobbli jiġi konness ma' back-end servers.
- Il-provvediment ta' serraturi fiżiċi lill-impjegati sabiex ikunu jistgħu fiżikament jipproteġu l-apparat mobbli li jużaw meta ma jkunx issorveljat.
- Regolamentazzjoni xierqa tal-użu tal-apparat barra mill-kumpanija.
- Regolamentazzjoni xierqa tal-użu tal-apparat fil-kumpanija.
- L-użu ta' software/applikazzjoni ta' MDM (Ġestjoni ta' Apparat Mobbli) u d-disponibbiltà ta' tħassir mill-bogħod.
- L-użu ta' mmaniġġar ċentralizzat tal-apparat bi drittijiet minimi għall-utenti finali sabiex jinstallaw is-software.
- L-installazzjoni ta' kontrolli fiżiċi tal-aċċess.
- L-evitar ta' ħżin ta' informazzjoni sensittiva fuq apparat mobbli jew fuq hard drives. Jekk ikun hemm bżonn li tiġi aċċessata s-sistema interna tal-kumpanija, għandhom jintużaw mezzi siguri bħal kif iddikjarat qabel.

6 IMPUSTAR ŻBALJAT

106. Is-sors tar-riskju huwa wkoll żball uman intern f'dan il-każ, iżda hawnhekk l-ebda azzjoni malizzjuża ma wasslet għall-ksur. Dan huwa r-riżultat ta' nuqqas ta' attenzjoni. Ftit li xejn jista' jsir mill-kontrollur wara li jkun seħħ, u għalhekk il-prevenzjoni hija saħansitra aktar importanti f'dawn il-każijiet milli f'tipi oħrajn ta' ksur.

6.1 KAŻ Nru 13: Żball fil-posta

Żewġ ordnijiet għal żraben ġew ippakkjati minn kumpanija tal-bejgħ bl-imnut. Minħabba żball uman, żewġ kontijiet tal-ippakkjar ġew imħallta bir-riżultat li kemm il-prodotti kif ukoll il-kontijiet rilevanti tal-ippakkjar intbagħtu lill-persuna żbaljata. Dan ifisser li ż-żewġ klijenti ħadu l-ordnijiet ta' xulxin, inklużi l-kontijiet tal-ippakkjar li fihom id-*data* personali. Wara li sar konxju mill-ksur, il-kontrollur tad-*data* sejjaħ lura l-ordnijiet u bagħathom lir-riċevituri t-tajba.

6.1.1 KAŻ Nru 13 - Miżuri preventivi u valutazzjoni tar-riskju

107. Il-kontijiet kien fihom id-*data* personali meħtieġa għal konsenja b'suċċess (l-isem, l-indirizz, flimkien mal-oġġett mixtri u l-prezz tiegħu). Huwa importanti li l-ewwel nett jiġi identifikat kif l-iżball uman seta' seħħ, u jekk bi kwalunkwe mod, setax jiġi evitat. Fil-każ partikolari deskritt ir-riskju huwa baxx, peress li ma kienet involuta l-ebda kategorija speċjali ta' *data* personali jew *data* oħra li l-abbuż tagħha jista' jwassal għal effetti negattivi sostanzjali, il-ksur ma huwiex riżultat ta' żball sistemiku min-naħa tal-kontrollur u huma kkonċernati żewġ individwi biss. Ma seta' jiġi identifikat l-ebda effett negattiv fuq l-individwi.

6.1.2 KAŻ Nru 13 – Mitigazzjoni u obbligi

108. Il-kontrollur għandu jipprovdi ritorn bla ħlas tal-oġġetti u tal-kontijiet li jakkumpanjawhom, u għandu jitlob ukoll lir-riċevituri żbaljati jeqirdu/jħassru l-kopji eventwali kollha tal-kontijiet li fihom id-*data* personali tal-persuna l-oħra.

109. Anke jekk il-ksur innifsu ma joħloqx riskju għoli għad-drittijiet u għal-libertajiet tal-individwi affettwati, u għalhekk il-komunikazzjoni lis-suġġetti tad-*data* ma hijiex obbligatorja mill-Artikolu 34 tal-GDPR, il-komunikazzjoni tal-ksur lilhom ma tistax tiġi evitata, peress li l-kooperazzjoni tagħhom hija meħtieġa sabiex jitnaqqas ir-riskju.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	X	X

6.2 KAŻ Nru 14: *Data* personali kunfidenzjali ħafna mibgħuta bil-posta bi żball

Id-dipartiment tal-impjiegi ta' uffiċċju tal-amministrazzjoni pubblika bagħat messaġġ permezz tal-posta elettronika – dwar taħriġ futur - lill-individwi rreġistrati fis-sistema tiegħu bħala persuni li qegħdin ifittxu impjieg. Bi żball, dokument li fih id-*data* personali ta' dawn il-persuni kollha li qegħdin ifittxu impjieg (l-isem, l-indirizz tal-posta elettronika, l-indirizz postali, in-numru tas-sigurtà soċjali) ġie mehmuż ma' din il-posta elettronika. In-numru ta' individwi affettwati huwa ta' aktar minn 60 000. Sussegwentement, l-uffiċċju kkuntattja lir-riċevituri kollha u talabhom iħassru l-messaġġ preċedenti u ma jużawx l-informazzjoni li tinsab fih.

6.2.1 KAŻ Nru 14 - Miżuri preventivi u valutazzjoni tar-riskju

110. Kellhom jiġu implimentati regoli aktar stretti relatati mal-bgħit ta' messaġġi bħal dawn. Jeħtieġ li tiġi kkunsidrata l-introduzzjoni ta' mekkaniżmi ta' kontroll addizzjonali.

111. In-numru ta' individwi affettwati huwa konsiderevoli, u l-involviment tan-numru tas-sigurtà soċjali tagħhom, flimkien ma' *data* oħra personali aktar bażika, ikompli jżid ir-riskju, li jista' jiġi identifikat bħala għoli[31]. Id-

[31] Għal gwida dwar operazzjonijiet ta' pproċessar li "*x'aktarx jirriżultaw f'riskju għoli*", ara n-nota 10 f'qiegħ il-paġna hawn fuq.

distribuzzjoni eventwali tad-*data* minn kwalunkwe wieħed mir-riċevituri ma tistax tiġi kkontrollata mill-kontrollur.

6.2.2 KAŻ Nru 14 – Mitigazzjoni u obbligi

112. Kif imsemmi qabel, il-mezzi sabiex jitnaqqsu b'mod effettiv ir-riskji ta' ksur simili huma limitati. Għalkemm il-kontrollur talab it-tħassir tal-messaġġ, ma jistax iġiegħel lir-riċevituri jagħmlu dan, u bħala konsegwenza, lanqas ma jista' jkun ċert li huma jikkonformaw mat-talba.

113. L-eżekuzzjoni tat-tliet azzjonijiet indikati hawn taħt għandha tkun evidenti f'każ bħal dan.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	✓	✓

6.3 KAŻ Nru 15: *Data* personali mibgħuta bil-posta bi żball

Lista ta' parteċipanti f'kors dwar l-Ingliż Legali li jsir f'lukanda għal ħamest ijiem tintbagħat bi żball lil 15-il parteċipant preċedenti tal-kors minflok lil-lukanda. Il-lista fiha l-ismijiet, l-indirizzi tal-posta elettronika u l-preferenzi alimentari tal-15-il parteċipant. Żewġ parteċipanti biss imlew il-preferenzi alimentari tagħhom, u ddikjaraw li huma intolleranti għal-lattożju. L-ebda wieħed mill-parteċipanti ma għandu identità protetta. Il-kontrollur jiskopri l-iżball minnufih wara li jibgħat il-lista u jinforma lir-riċevituri dwar l-iżball u jitlob li titħassar il-lista.

6.3.1 KAŻ Nru 15 - Miżuri preventivi u valutazzjoni tar-riskju

114. Kellhom jiġu implimentati regoli stretti għall-bgħit ta' messaġġi li jkun fihom *data* personali. Jeħtieġ li tiġi kkunsidrata l-introduzzjoni ta' mekkaniżmi ta' kontroll addizzjonali.

115. Ir-riskji li jirriżultaw min-natura, mis-sensittività, mill-volum u mill-kuntest tad-*data* personali huma baxxi. Id-*data* personali tinkludi *data* sensittiva dwar il-preferenzi alimentari ta' tnejn mill-parteċipanti. Anke jekk l-informazzjoni li xi ħadd ma jittollerax il-lattożju hija *data* relatata mas-saħħa, ir-riskju li din id-*data* tintuża b'mod detrimentali għandu jitqies relattivament baxx. Filwaqt li fil-każ ta' *data* relatata mas-saħħa, normalment jiġi preżunt li l-ksur x'aktarx jirriżulta f'riskju għoli għas-suġġett tad-*data*[32], fl-istess ħin f'dan il-każ partikolari ma jista' jiġi identifikat l-ebda riskju li l-ksur iwassal għal ksur fiżiku, jew għal danni materjali jew mhux materjali tas-suġġett tad-*data* minħabba d-divulgazzjoni mhux awtorizzata tal-informazzjoni dwar l-intolleranza għal-lattożju. Għall-kuntrarju ta' xi preferenzi oħrajn tal-ikel, l-intolleranza għal-lattożju normalment ma tistax tkun marbuta ma' xi twemmin reliġjuż jew filosofiku. Il-kwantità tad-*data* li fuqha tkun seħħet vjolazzjoni u n-numru ta' suġġetti tad-*data* affettwati huma baxxi ħafna wkoll.

6.3.2 KAŻ Nru 15 – Mitigazzjoni u obbligi

116. Fil-qosor, jista' jiġi ddikjarat li l-ksur ma kellu l-ebda effett sinifikanti fuq is-suġġetti tad-*data*. Il-fatt li l-kontrollur ikkuntattja lir-riċevituri immedjatament wara li sar konxju mill-iżball jista' jitqies bħala fattur ta' mitigazzjoni.

117. Jekk tintbagħat posta elettronika lil riċevitur żbaljat/mhux awtorizzat, huwa rrakkomandat li l-kontrollur tad-*data* jibgħat posta elettronika ta' segwitu lir-riċevituri mhux intenzjonati u jagħmel użu mill-funzjoni Bcc li

[32] Ara l-Linji Gwida WP 250, p. 23.

titlob skuża, u tagħti struzzjonijiet li l-posta elettronika offensiva għandha titħassar, u tinforma lir-riċevituri li ma għandhomx id-dritt li jkomplu jużaw l-indirizzi tal-posta elettronika identifikati lilhom.

118. Minħabba dawn il-fatti, dan il-ksur tad-*data* x'aktarx li ma jirriżultax f'riskju għad-drittijiet u l-libertajiet tas-suġġetti tad-*data*, u b'hekk ma kienet meħtieġa l-ebda notifika lill-SA jew lis-suġġetti tad-*data* kkonċernati. Madankollu, dan il-ksur tad-*data* jrid jiġi ddokumentat ukoll f'konformità mal-Artikolu 33(5).

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	X	X

6.4 KAŻ Nru 16: Żball fil-posta

Grupp tal-assigurazzjoni joffri assigurazzjonijiet tal-karozzi. Sabiex jagħmel dan, jibgħat politiki ta' kontribuzzjoni aġġustati regolarment bil-posta. Minbarra l-isem u l-indirizz tad-detentur tal-polza, l-ittra jkun fiha n-numru tar-reġistrazzjoni tal-vettura mingħajr numri moħbija, ir-rati tal-assigurazzjoni tas-sena tal-assigurazzjoni attwali u ta' wara, il-kilometraġġ annwali approssimattiv u d-data tat-twelid tad-detentur tal-polza. Ma hemmx *data* inkluża relatata mas-saħħa skont l-Artikolu 9 tal-GDPR, *data* dwar il-ħlas (dettalji bankarji), *data* ekonomika u finanzjarja.

L-ittri huma ppakkjati minn magni awtomatizzati li jippakkjaw. Minħabba żball mekkaniku, żewġ ittri għal detenturi ta' poloz differenti iddaħħlu f'envelop wieħed u ntbagħtu lil detentur ta' polza wieħed permezz ta' ittra postali. Id-detentur tal-polza fetaħ l-ittra d-dar u ta ħarsa lejn l-ittra tiegħu li tkun intbagħtet b'mod korrett kif ukoll lejn l-ittra li tkun intbagħtet b'mod żbaljat minn detentur ta' polza ieħor.

6.4.1 KAŻ Nru 16 - Miżuri preventivi u valutazzjoni tar-riskju

119. L-ittra mwassla b'mod żbaljat fiha l-isem, l-indirizz, id-data tat-twelid, in-numru tar-reġistrazzjoni tal-vettura mhux mgħotti u l-klassifikazzjoni tar-rata tal-assigurazzjoni tas-sena attwali u s-sena ta' wara. L-effetti fuq il-persuna affettwata għandhom jitqiesu bħala medji, peress li informazzjoni mhux disponibbli pubblikament, bħad-data tat-twelid jew in-numri tar-reġistrazzjoni tal-vettura mhux moħbija, u d-dettalji dwar iż-żieda fir-rati tal-assigurazzjoni, jiġu ddivulgati lir-riċevitur mhux awtorizzat. Il-probabbiltà ta' użu ħażin ta' din id-*data* hija vvalutata bħala bejn baxxa u medja. Madankollu, filwaqt li ħafna riċevituri probabbilment se jarmu l-ittra riċevuta b'mod żbaljat fiż-żibel, f'każijiet individwali ma jistax jiġi eskluż kompletament li l-ittra ma tittellax fuq networks soċjali jew li d-detentur tal-polza ma jiġix ikkuntattjat.

6.4.2 KAŻ Nru 16 – Mitigazzjoni u obbligi

120. Il-kontrollur għandu jirritorna d-dokument oriġinali bi spejjeż tiegħu. Ir-riċevitur żbaljat għandu jiġi informat ukoll li huwa ma għandux juża ħażin l-informazzjoni li tinqara.

121. Probabbilment qatt ma huwa se jkun possibbli li jiġi evitat kompletament żball fil-konsenja postali f'posta tal-massa bl-użu ta' magni kompletament awtomatizzati. Madankollu, fil-każ ta' frekwenza akbar, huwa meħtieġ li jiġi vverifikat jekk il-magni li jippakkjaw humiex stabbiliti u miżmuma b'mod korrett biżżejjed, jew jekk xi kwistjoni sistemika oħra twassalx għal tali ksur.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	✓	X

6.5 Miżuri organizzazzjonali u tekniċi għall-prevenzjoni/għall-mitigazzjoni tal-impatti ta' posta żbaljata

122. Kombinament tal-miżuri msemmija hawn taħt – applikati skont il-karatteristiċi uniċi tal-każ – għandu jgħin sabiex jitnaqqas iċ-ċans li jerġa' jseħħ ksur simili.

123. Miżuri rakkomandati:

(*Il-lista tal-miżuri li ġejjin bl-ebda mod ma hija esklużiva jew komprensiva. Pjuttost, l-għan huwa li jiġu pprovduti ideat għall-prevenzjoni u soluzzjonijiet possibbli. Kull attività ta' pproċessar hija differenti, għalhekk il-kontrollur għandu jieħu d-deċiżjoni dwar liema miżuri huma l-aktar adatti għas-sitwazzjoni partikolari.*)

- L-istabbiliment ta' standards preċiżi – mingħajr ebda lok għal interpretazzjoni - sabiex jintbagħtu l-ittri/l-posta elettronika.
- Taħriġ adegwat għall-persunal dwar kif jintbagħtu l-ittri/l-posta elettronika.
- Meta tintbagħat posta elettronika lil diversi riċevituri, dawn għandhom jiġu elenkati fit-taqsima Bcc b'mod prestabbilit.
- Tkun meħtieġa konferma addizzjonali meta tintbagħat posta elettronika lil diversi riċevituri u dawn ma jkunux elenkati fit-taqsima Bcc.
- L-applikazzjoni tal-prinċipju ta' erba' għajnejn.
- L-indirizzar awtomatiku minflok manwali, b'*data* estratta minn bażi ta' *data* disponibbli u aġġornata; is-sistema ta' indirizzar awtomatiku għandha tiġi rieżaminata regolarment sabiex tivverifika l-iżbalji moħbija u l-konfigurazzjonijiet żbaljati.
- L-applikazzjoni tal-funzjoni message delay (eż. il-messaġġ jista' jitħassar/jiġi editjat f'ċertu perjodu ta' żmien wara li tikklikkja l-buttuna).
- Id-diżattivazzjoni tal-funzjoni autocomplete meta jkunu qegħdin jinkitbu l-indirizzi tal-posta elettronika.
- Sessjonijiet ta' sensibilizzazzjoni dwar l-aktar żbalji komuni li jwasslu għal ksur ta' *data* personali.
- Sessjonijiet ta' taħriġ u manwali dwar kif għandhom jiġu ttrattati inċidenti li jwasslu għal ksur ta' *data* personali u min għandu jiġi informat (bl-involviment tad-DPO).

7 KAŻIJIET OĦRAJN – INĠINERIJA SOĊJALI

7.1 KAŻ Nru 17: Serq tal-identità

Iċ-ċentru ta' kuntatt ta' kumpanija tat-telekomunikazzjoni irċieva telefonata mingħand xi ħadd li jagħmilha ta' klijent. L-allegat klijent talab lill-kumpanija sabiex tibdel l-indirizz tal-posta elettronika li fuqu jirċievi l-informazzjoni dwar il-kontijiet minn dakinhar 'il quddiem. Il-ħaddiem taċ-ċentru ta' kuntatt ivvalida l-identità tal-klijent billi talab ċerta *data* personali, kif definit mill-proċeduri tal-kumpanija. Min iċempel indika b'mod korrett in-numru fiskali u l-indirizz postali tal-klijent rikjest (minħabba li kellu aċċess għal dawn l-elementi). Wara l-validazzjoni, l-operatur jagħmel il-bidla mitluba u, minn dakinhar 'il quddiem, l-informazzjoni dwar il-kontijiet bdiet tintbagħat lill-indirizz elettroniku l-ġdid. Il-proċedura ma tipprevedi l-ebda notifika lill-kuntatt elettroniku preċedenti. Ix-xahar ta' wara, il-klijent leġittimu ikkuntattja lill-kumpanija sabiex jistaqsi għaliex ma kienx qiegħed jirċievi l-kontijiet fuq l-indirizz tal-posta elettronika tiegħu, u jiċħad kwalunkwe sejħa minnu li titlob il-bidla tal-kuntatt ta' posta elettronika. Aktar tard, il-kumpanija ntebħet li l-informazzjoni ntbagħtet lil utent illeġittimu u sejħet lura l-bidla.

7.1.1 KAŻ Nru 17 - Valutazzjoni tar-riskju, mitigazzjoni u obbligi

124. Dan il-każ iservi bħala eżempju tal-importanza ta' miżuri preventivi. Il-ksur, minn aspett ta' riskju, jippreżenta livell għoli ta' riskju33, peress li d-*data* dwar il-kontijiet tista' tagħti informazzjoni dwar il-ħajja privata tas-suġġett tad-*data* (eż. drawwiet, kuntatti) u jista' jwassal għal ħsara materjali (eż. is-segwiment ta' persuna bil-moħbi, riskju għall-integrità fiżika). Id-*data* personali miksuba matul dan l-attakk tista' tintuża wkoll sabiex jiġi ffaċilitat l-akkwist tal-kontijiet f'din l-organizzazzjoni jew jiġu sfruttati aktar miżuri ta' awtentikazzjoni f'organizzazzjonijiet oħrajn. Meta jitqiesu dawn ir-riskji, il-miżura ta' awtentikazzjoni "xierqa" għandha tissodisfa standard għoli, skont liema *data* personali tista' tiġi pproċessata bħala riżultat tal-awtentikazzjoni.

125. B'riżultat ta' dan, kemm notifika lill-SA kif ukoll komunikazzjoni lis-suġġett tad-*data* huma meħtieġa mill-kontrollur.

126. Huwa ċar li l-proċess preċedenti ta' validazzjoni tal-klijent għandu jiġi rfinat fid-dawl ta' dan il-każ. Il-metodi użati għall-awtentikazzjoni ma kinux biżżejjed. Il-parti malizzjuża kienet kapaċi tagħmilha tal-utent intenzjonat permezz tal-użu ta' informazzjoni disponibbli għall-pubbliku u informazzjoni li kellha aċċess għaliha b'mod ieħor.

127. L-użu ta' dan it-tip ta' awtentikazzjoni statika bbażata fuq l-għarfien (fejn it-tweġiba ma tinbidilx, u fejn l-informazzjoni ma tkunx "sigrieta" bħalma jkun il-każ għal password) ma huwiex rakkomandat.

128. Minflok, l-organizzazzjoni għandha tuża forma ta' awtentikazzjoni li tirriżulta fi grad għoli ta' fiduċja li l-utent awtentikat huwa l-persuna maħsuba, u mhux xi ħadd ieħor. L-introduzzjoni ta' metodu ta' awtentikazzjoni b'diversi fatturi barra mill-banda għandha ssolvi l-problema, eż. sabiex tiġi vverifikata t-talba għal bidla, billi tintbagħat talba ta' konferma lill-kuntatt preċedenti; jew iż-żieda ta' mistoqsijiet addizzjonali u l-ħtieġa ta' informazzjoni viżibbli biss fuq il-kontijiet preċedenti. Hija r-responsabbiltà tal-kontrollur li jiddeċiedi liema miżuri jintroduċi, peress li huwa jaf id-dettalji u r-rekwiżiti tal-operazzjoni interna tiegħu l-aktar.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	✓	✓

7.2 KAŻ Nru 18: Eksfiltrazzjoni tal-posta elettronika

[33] Għal gwida dwar operazzjonijiet ta' pproċessar li "*x'aktarx jirriżultaw f'riskju għoli*", ara n-nota 10 f'qiegħ il-paġna hawn fuq.

Katina tal-hypermarkets identifikat, 3 xhur wara l-konfigurazzjoni tagħha, li xi kontijiet tal-posta elettronika ġew mibdula u li nħolqu regoli sabiex kwalunkwe posta elettronika li jkun fiha ċerti espressjonijiet (eż. “fattura”, “ħlas”, “bank wiring”, “awtentikazzjoni tal-karti ta’ kreditu”, “dettalji tal-kont bankarju”) tiġi ttrasferita f’folder mhux użat u tintbagħat ukoll lil indirizz elettroniku estern. Barra minn hekk, sa dak iż-żmien, kien diġà sar attakk ta’ inġinerija soċjali, jiġifieri, l-attakkant, filwaqt li għamilha ta’ fornitur, bidel id-dettalji tal-kont bankarju tal-fornitur f’ismu. Fl-aħħar nett, sa dak iż-żmien, intbagħtu diversi fatturi foloz li kienu jinkludu d-dettall tal-kont bankarju l-ġdid. Is-sistema ta’ monitoraġġ tal-pjattaforma tal-posta elettronika spiċċat tagħti twissija dwar il-folders. Il-kumpanija ma setgħetx tidentifika kif l-attakkant seta’ jikseb aċċess għall-kontijiet tal-posta elettronika, iżda assumiet li posta elettronika infettata kienet ir-raġuni għall-għoti ta’ aċċess lill-grupp ta’ utenti responsabbli għall-pagamenti.

Minħabba t-trażmissjoni ta’ posta elettronika bbażata fuq il-keyword, l-attakkant irċieva informazzjoni dwar 99 impjegat: l-isem u l-paga ta’ xahar partikolari ta’ 89 suġġett tad-*data*; l-isem, l-istatus ċivili, in-numru ta’ tfal, il-paga, is-sigħat tax-xogħol u l-bqija tal-informazzjoni li tinstab fir-riċevuta tas-salarju ta’ 10 impjegati li l-kuntratti tagħhom ġew konklużi. Il-kontrollur innotifika biss lill-10 impjegati li jappartjenu għall-grupp tal-aħħar.

7.2.1 KAŻ Nru 18 - Valutazzjoni tar-riskju, mitigazzjoni u obbligi

129. Anke jekk l-attakkant probabbilment ma kienx qiegħed jimmira li jiġbor *data* personali, peress li l-ksur jista’ jwassal kemm għal ħsara materjali (eż. telf finanzjarju) kif ukoll għal ħsara mhux materjali (eż. serq tal-identità jew frodi), jew peress li d-*data* tista’ tintuża sabiex tiffaċilita attakki oħrajn (eż. phishing), il-ksur tad-*data* personali x’aktarx li jirriżulta f’riskju għoli għad-drittijiet u għal-libertajiet tal-persuni fiżiċi. Għalhekk, il-ksur għandu jiġi kkomunikat lid-99 impjegat kollha u mhux biss lill-10 impjegati li l-informazzjoni dwar is-salarju tagħhom kienet ġiet żvelata.

130. Wara li sar konxju mill-ksur, il-kontrollur sforza bidla fil-password għall-kontijiet kompromessi, imblokka l-bgħit ta’ posta elettronika lill-kont tal-posta elettronika tal-attakkant, innotifika lill-fornitur tas-servizz bl-indirizz tal-posta elettronika użat mill-attakkant rigward l-azzjonijiet tiegħu jew tagħha, neħħa r-regoli stabbiliti mill-attakkant u rfina t-twissijiet tas-sistema ta’ monitoraġġ sabiex jagħtu twissija hekk kif tinħoloq regola awtomatika. Alternattivament, il-kontrollur jista’ jneħħi d-dritt tal-utenti li jistabbilixxu regoli ta’ trażmissjoni, u t-tim tas-servizzi tal-IT seta’ jagħmel dan biss fuq talba jew jista’ jintroduċi politika li l-utenti għandhom jivverifikaw u jirrapportaw ir-regoli stabbiliti fil-kontijiet tagħhom darba fil-ġimgħa jew aktar ta’ spiss, f’oqsma li jittrattaw id-*data* finanzjarja.

131. Il-fatt li ksur jista’ jseħħ u ma jiġix skopert għal tant żmien u l-fatt li, fi żmien itwal, l-inġinerija soċjali setgħet intużat sabiex tinbidel aktar *data*, enfasizzaw problemi sinifikanti fis-sistema tas-sigurtà tal-IT tal-kontrollur. Dawn għandhom jiġu indirizzati mingħajr dewmien, pereżempju permezz ta’ enfasi fuq ir-rieżamijiet tal-awtomatizzazzjoni u l-kontrolli tat-tibdil, u l-miżuri ta’ detezzjoni u ta’ rispons għall-inċidenti. Il-kontrolluri li jittrattaw *data* sensittiva, informazzjoni finanzjarja, eċċ. għandhom responsabbiltà akbar f’termini ta’ provvediment ta’ sigurtà adegwata tad-*data*.

Azzjonijiet meħtieġa abbażi tar-riskji identifikati		
Dokumentazzjoni interna	Notifika lill-SA	Komunikazzjoni lis-suġġetti tad-*data*
✓	✓	✓