Linji Gwida

Linji Gwida 9/2022 dwar in-notifika ta' ksur ta' *data* personali skont il-GDPR

Verżjoni 2.0

Adottati fit-28 ta' Marzu 2023

This language version has not yet been proofread.

Rekord tal-verżjonijiet

Verżjoni 1.0	10 ta' Ottubru 2022	Adozzjoni tal-Linji Gwida (verżjoni aġġornata tal-linji gwida preċedenti WP250 (rev.01) adottati mill-Grupp ta' Ħidma 29 u approvati mill-EDPB fil-25 ta' Mejju 2018) għal konsultazzjoni pubblika mmirata.
Verżjoni 2.0	28 ta' Marzu 2023	Adozzjoni tal-Linji Gwida wara l-konsultazzjoni pubblika mmirata dwar is-suġġett tan-notifika ta' ksur tad-*data* għall-kontrolluri mhux stabbiliti fiż-ŻEE.

WERREJ

Il-Bord Ewropew għall-Protezzjoni tad-*Data*

Wara li kkunsidra l-Artikolu 70(1)(e) u (l) 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", General Data Protection Regulation),

Wara li kkunsidra l-Ftehim ŻEE u b'mod partikolari l-Anness XI u l-Protokoll 37 tiegħu, kif emendat 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-Linji Gwida tal-Grupp ta' Ħidma tal-Artikolu 29 dwar in-notifika ta' ksur ta' *data* personali skont ir-Regolament 2016/679, WP250 rev.01,

ADOTTA L-LINJI GWIDA LI ĠEJJIN

0 DAĦLA

1. Fit-3 ta' Ottubru 2017, il-Grupp ta' Ħidma 29 (minn hawn 'il quddiem "WP29", Working Party 29) adotta l-Linji Gwida tiegħu dwar notifika ta' ksur ta' *data* personali skont ir-Regolament 2016/679 (WP250 rev.01)[2], li ġew approvati mill-Bord Ewropew għall-Protezzjoni tad-*Data* (minn hawn' il quddiem "EDPB", European Data Protection Board) fl-ewwel laqgħa plenarja tiegħu[3]. Dan id-dokument huwa verżjoni kemxejn aġġornata ta' dawk il-linji gwida. Kwalunkwe referenza għal-Linji Gwida tad-WP29 dwar in-notifika ta' ksur ta' *data* personali skont ir-Regolament 2016/679 (WP250 rev.01) minn issa 'l quddiem għandha tiġi interpretata bħala referenza għal dawn il-Linji Gwida 9/2022 tal-EDPB.
2. L-EDPB innota li kien hemm bżonn li jiġu ċċarati r-rekwiżiti ta' notifika dwar il-ksur ta' *data* personali fi stabbilimenti mhux tal-UE. Il-paragrafu dwar din il-kwistjoni ġie rivedut u aġġornat, filwaqt li l-bqija tad-dokument ma nbidilx, ħlief għal bidliet editorjali. Ir-reviżjoni tikkonċerna, b'mod aktar speċifiku, il-paragrafu 73 fit-Taqsima II.C.2 ta' dan id-dokument.

INTRODUZZJONI

3. Il-GDPR jintroduċi r-rekwiżit biex ksur ta' *data* personali (minn hawn 'il quddiem "ksur") jiġi notifikat lill-awtorità superviżorja nazzjonali kompetenti[4] (jew, fil-każ ta' ksur transfruntier, lill-awtorità prinċipali) u, f'ċerti każijiet, biex il-ksur jiġi komunikat lill-individwi li d-*data* personali tagħhom kienet affettwata mill-ksur.
4. L-obbligi ta' notifika f'każijiet ta' ksur kienu jeżistu għal ċerti organizzazzjonijiet, bħall-fornituri ta' servizzi tal-komunikazzjoni elettronika disponibbli pubblikament (kif speċifikat fid-Direttiva

[1] Ir-referenzi għal "Stati Membri" li jsiru tul dan id-dokument għandhom jinftiehmu bħala referenzi għal "Stati Membri taż-ŻEE".
[2] Il-Linji Gwida tad-WP29 dwar in-notifika ta' ksur ta' *data* personali skont ir-Regolament 2016/679 (WP250 rev.01) (riveduti u aġġornati l-aħħar fis-6 ta' Frar 2018), disponibbli fuq https://ec.europa.eu/newsroom/article29/items/612052.
[3] Ara https://www.edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_mt.
[4] Ara l-Artikolu 4(21) tal-GDPR.

2009/136/KE u fir-Regolament (UE) Nru 611/2013)[5]. Kien hemm ukoll xi Stati Membri li diġà kellhom l-obbligu ta' notifika ta' ksur nazzjonali tagħhom stess. Dan seta' jinkludi l-obbligu ta' notifika ta' ksur li jinvolvi kategoriji ta' kontrolluri minbarra l-forniturі ta' servizzi tal-komunikazzjoni elettronika disponibbli pubblikament (pereżempju fil-Ġermanja u fl-Italja), jew obbligu ta' rapportar ta' kull ksur li jinvolvi *data* personali (bħal fin-Netherlands). Stati Membri oħra seta' kellhom Kodiċijiet ta' Prattika rilevanti (pereżempju fl-Irlanda[6]). Filwaqt li għadd ta' awtoritajiet tal-protezzjoni tad-*data* tal-UE ħeġġew lill-kontrolluri jirrapportaw ksur, id-Direttiva dwar il-Protezzjoni tad-*Data* 95/46/KE[7], li l-GDPR issostitwixxa, ma kienx fiha obbligu speċifiku ta' notifika ta' ksur u, għaldaqstant, rekwiżit bħal dan kien ġdid għal ħafna organizzazzjonijiet. Il-GDPR jagħmel in-notifika obbligatorja għall-kontrolluri kollha sakemm ma jkunx improbabbli li ksur jirriżulta f'riskju għad-drittijiet u għal-libertajiet tal-individwi[8]. Il-proċessuri għandhom ukoll rwol importanti x'jaqdu u dawn iridu jinnotifikaw kwalunkwe ksur lill-kontrollur tagħhom[9].

5. L-EDPB iqis li r-rekwiżit ta' notifika għandu għadd ta' benefiċċji. Meta jinnotifikaw lill-awtorità superviżorja, il-kontrolluri jistgħu jiksbu pariri dwar jekk l-individwi affettwati għandhomx bżonn jiġu informati. Tabilħaqq, l-awtorità superviżorja tista' tordna lill-kontrollur jinforma lil dawk l-individwi dwar il-ksur[10]. Il-komunikazzjoni ta' ksur lill-individwi tippermetti li l-kontrollur jipprovdi informazzjoni dwar ir-riskji ppreżentati bħala riżultat tal-ksur u l-passi li dawk l-individwi jistgħu jieħdu biex jipproteġu lilhom infushom mill-konsegwenzi potenzjali tiegħu. L-enfasi ta' kwalunkwe pjan ta' rispons għal ksur għandha tkun fuq il-protezzjoni tal-individwi u tad-*data* personali tagħhom. Konsegwentement, in-notifika ta' ksur għandha titqies li hi għodda li ssaħħaħ il-konformità b'rabta mal-protezzjoni ta' *data* personali. Fl-istess ħin, ta' min jinnota li, skont l-Artikolu 83 tal-GDPR, nuqqas ta' rapportar ta' ksur lil individwu jew lil awtorità superviżorja jista' jfisser li tkun applikabbli sanzjoni possibbli għall-kontrollur.

6. Għaldaqstant, il-kontrolluri u l-proċessuri huma mħeġġa jippjanaw bil-lest u jimplimentaw proċessi biex ikunu jistgħu jidentifikaw u jikkontjenu minnufih ksur, biex jivvalutaw ir-riskju għall-individwi[11], u mbagħad biex jiddeterminaw jekk hemmx bżonn li jinnotifikaw lill-awtorità superviżorja kompetenti, u biex jikkomunikaw il-ksur lill-individwi kkonċernati meta jkun hemm bżonn. In-notifika lill-awtorità superviżorja għandha tagħmel parti minn dak il-pjan ta' rispons għal inċident.

7. Il-GDPR fih dispożizzjonijiet dwar meta ksur irid jiġi notifikat, u lil min, kif ukoll dwar x'informazzjoni għandha tiġi pprovduta bħala parti min-notifika. L-informazzjoni meħtieġa għan-notifika tista' tiġi pprovduta f'fażijiet, iżda fi kwalunkwe każ il-kontrolluri għandhom jaġixxu fuq kwalunkwe ksur fil-pront.

8. Fl-Opinjoni 03/2014 tiegħu dwar in-notifika ta' ksur ta' *data* personali[12], id-WP29 ipprovda gwida lill-kontrolluri biex jgħinhom jiddeċiedu meta jinnotifikaw lis-suġġetti tad-*data* f'każ ta' ksur. L-opinjoni kkunsidrat l-obbligu tal-forniturі ta' komunikazzjonijiet elettroniċi rigward id-Direttiva 2002/58/KE u

---

[5] Ara http://eur-lex.europa.eu/legal-content/MT/TXT/?uri=celex:32009L0136 u http://eur-lex.europa.eu/legalcontent/MT/TXT/?uri=CELEX%3A32013R0611

[6] Ara https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[7] Ara http://eur-lex.europa.eu/legal-content/MT/TXT/?uri=celex:31995L0046

[8] Id-drittijiet minquxin fil-Karta tad-Drittijiet Fundamentali tal-UE, disponibbli fuq http://eurlex.europa.eu/legal-content/MT/TXT/?uri=CELEX:12012P/TXT

[9] Ara l-Artikolu 33(2) tal-GDPR. Dan hu simili fil-kunċett għall-Artikolu 5 tar-Regolament (UE) Nru 611/2013 li jiddikjara li fornitur li jidħol f'kuntratt biex jipprovdi parti minn servizz tal-komunikazzjoni elettronika (mingħajr ma jkollu relazzjoni kuntrattwali diretta mal-abbonati) hu obbligat jinnotifika lill-fornitur kontraenti f'każ ta' ksur ta' *data* personali.

[10] Ara l-Artikoli 34(4) u 58(2)(e) tal-GDPR.

[11] Dan jista' jiġi ġgurat skont ir-rekwiżit ta' monitoraġġ u ta' rieżami ta' DPIA (data protection impact assessment), li hu meħtieġ għal operazzjonijiet ta' proċessar li aktarx li jirriżultaw f'riskju għoli għad-drittijiet u għal-libertajiet ta' persuni fiżiċi (l-Artikolu 35(1) u (11)).

[12] Ara l-Opinjoni 03/2014 tad-WP29 dwar in-notifika ta' ksur ta' *data* personali http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

tat eżempji minn diversi setturi, fil-kuntest ta' dak li dak iż-żmien kien abbozz tal-GDPR, u ppreżentat il-prattiki tajbin għall-kontrolluri kollha.

9. Il-Linji Gwida kurrenti jispjegaw ir-rekwiżiti obbligatorji tal-GDPR ta' notifika u ta' komunikazzjoni ta' ksur u wħud mill-passi li l-kontrolluri u l-proċessuri jistgħu jieħdu biex jissodisfaw dawn l-obbligi. Huma jagħtu wkoll eżempji ta' diversi tipi ta' ksur u min ikollu jiġi nnotifikat f'xenarji differenti.

I. NOTIFIKA TA' KSUR TA' *DATA* PERSONALI SKONT IL-GDPR

A. Kunsiderazzjonijiet dwar is-sigurtà bażika

10. Wieħed mir-rekwiżiti tal-GDPR hu li, billi jintużaw miżuri tekniċi u organizzattivi xierqa, id-*data* personali għandha tiġi proċessata b'mod li jiżgura s-sigurtà xierqa tad-*data* personali, inkluża l-protezzjoni kontra proċessar mhux awtorizzat jew illegali u kontra telf aċċidentali, qerda jew ħsara[13].

11. Għalhekk, il-GDPR jeħtieġ li kemm il-kontrolluri kif ukoll il-proċessuri jkollhom fis-seħħ miżuri tekniċi u organizzattivi xierqa biex jiżguraw livell ta' sigurtà xieraq għar-riskju miġjub għad-*data* personali li tiġi proċessata. Dawn għandhom iqisu l-istat attwali, il-kostijiet tal-implimentazzjoni u n-natura, il-kamp ta' applikazzjoni, il-kuntest u l-iskopijiet tal-ipproċessar, kif ukoll ir-riskju ta' probabbiltà u ta' severità li tvarja għad-drittijiet u għal-libertajiet tal-persuni fiżiċi[14]. Barra minn hekk, il-GPDR jeħtieġ li l-miżuri xierqa kollha ta' protezzjoni teknoloġika u organizzattivi jkunu fis-seħħ biex jiġi stabbilit minnufih jekk seħħx ksur, li mbagħad jiddetermina jekk jiskattax l-obbligu ta' notifika[15].

12. Konsegwentement, element importanti ta' kwalunkwe politika dwar is-sigurtà tad-*data* hu li, fejn possibbli, din tkun kapaċi tipprevjeni ksur u, fejn dan iseħħ xorta waħda, tirreaġixxi għalih fil-pront.

B. X'inhu ksur ta' *data* personali?

1. Definizzjoni

13. Bħala parti minn kwalunkwe tentattiv biex jiġi indirizzat ksur, il-kontrollur l-ewwel għandu jkun kapaċi jagħrfu. Il-GDPR jiddefinixxi "ksur ta' *data* personali" fl-Artikolu 4(12) kif ġej:

> "*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*".

14. X'nifhmu b'"qerda" ta' *data* personali għandu jkun pjuttost ċar: din iseħħ meta d-*data* ma tibqax teżisti, jew ma tibqax teżisti f'forma li hi ta' ebda użu għall-kontrollur. "Ħsara" għandha tkun relattivament ċara wkoll: din iseħħ meta d-*data* personali titbiddel, tiġi mbagħbsa, jew ma tibqax kompluta. F'termini ta' "telf" ta' *data* personali, dan għandu jiġi interpretat bħala l-possibbiltà li d-*data* tista' tkun għadha teżisti, iżda l-kontrollur tilef il-kontroll jew l-aċċess għaliha, jew ma għadhiex fil-pussess tiegħu. Finalment, proċessar mhux awtorizzat jew illegali jista' jinkludi divulgazzjoni ta' *data* personali lil (jew l-aċċess minn) riċevituri li mhumiex awtorizzati jirċievu (jew jaċċessaw) id-*data*, jew kwalunkwe forma oħra ta' proċessar li tikser il-GDPR.

> **Eżempju**
>
> Eżempju ta' telf ta' *data* personali jista' jinkludi każ li fih jintilef jew jinsteraq apparat li fih kopja tal-bażi ta' *data* tal-klijenti ta' kontrollur. Eżempju ieħor ta' telf jista' jkun meta l-unika kopja ta' sett ta'

[13] Ara l-Artikoli 5(1)(f) u 32 tal-GDPR.
[14] L-Artikolu 32; ara wkoll il-Premessa 83 tal-GDPR.
[15] Ara l-Premessa 87 tal-GDPR.

data personali tiġi kriptata b'software ta' riskatt, jew tiġi kriptata mill-kontrollur permezz ta' kjavi li ma għadhiex fil-pussess tiegħu.

15. Dak li għandu jkun ċar hu li ksur hu tip ta' inċident tas-sigurtà. Madankollu, kif indikat mill-Artikolu 4(12), il-GDPR japplika biss meta jkun hemm ksur ta' *data* personali. Il-konsegwenza ta' tali ksur hi li l-kontrollur ma jkunx jista' jiżgura l-konformità mal-prinċipji relatati mal-proċessar ta' *data* personali kif spjegat fl-Artikolu 5 tal-GDPR. Dan jixħet dawl fuq id-differenza bejn inċident tas-sigurtà u ksur ta' *data* personali – essenzjalment, filwaqt li kull ksur ta' *data* personali hu inċident tas-sigurtà, mhux l-inċidenti tas-sigurtà kollha bilfors ikunu ksur ta' *data* personali[16].

16. L-effetti avversi potenzjali ta' ksur fuq l-individwi huma kkunsidrati hawn taħt.

2. Tipi ta' ksur ta' *data* personali

17. Fl-Opinjoni 03/2014 tiegħu dwar in-notifika ta' ksur, id-WP29 spjega li l-ksur jista' jiġi kategorizzat skont it-tliet prinċipji ferm magħrufa li ġejjin dwar is-sigurtà tal-informazzjoni[17]:

    - "**Ksur tal-kunfidenzjalità**" - meta jkun hemm divulgazzjoni mhux awtorizzata jew aċċidentali ta' *data* personali, jew aċċess mhux awtorizzat għaliha.

    - "**Ksur tal-integrità**" - meta jkun hemm alterazzjoni mhux awtorizzata jew aċċidentali ta' *data* personali.

    - "**Ksur tad-disponibbiltà**" - meta jkun hemm telf aċċidentali jew mhux awtorizzat ta' aċċess[18] għal *data* personali, jew il-qerda aċċidentali jew mhux awtorizzata tagħha.

18. Ta' min jinnota wkoll li, skont iċ-ċirkustanzi, ksur jista' jikkonċerna l-kunfidenzjalità, l-integrità u d-disponibbiltà ta' *data* personali fl-istess ħin, kif ukoll kwalunkwe taħlita ta' dawn.

19. Filwaqt li d-determinazzjoni ta' jekk seħħx ksur tal-kunfidenzjalità jew tal-integrità hi relattivament ċara, jekk seħħx ksur tad-disponibbiltà jista' jkun inqas ovvju. Ksur dejjem jitqies bħala ksur tad-disponibbiltà meta jkun seħħ telf permanenti ta' *data* personali jew il-qerda tagħha.

Eżempju

Eżempji ta' telf ta' disponibbiltà jinkludu każijiet li fihom id-*data* titħassar b'mod aċċidentali jew minn persuna mhux awtorizzata, jew, fl-eżempju ta' *data* kriptata b'mod sigur, tintilef il-kjavi dekriptografika. F'każ li l-kontrollur ma jkunx jista' jerġa' jirrestawra l-aċċess għad-*data*, pereżempju, minn kopja ta' riżerva, dan jitqies li hu telf permanenti tad-disponibbiltà.

Telf tad-disponibbiltà jista' jseħħ ukoll meta jkun hemm interruzzjoni sinifikanti fis-servizz normali ta' organizzazzjoni, pereżempju qtugħ tad-dawl jew attakk li jwaqqaf is-servizz, li trendi d-*data* personali indisponibbli.

---

[16] Ta' min jinnota li inċident tas-sigurtà mhuwiex limitat għal mudelli ta' theddid li fihom isir attakk fuq organizzazzjoni minn sors estern, iżda jinkludi inċidenti mill-proċessar intern li jiksru l-prinċipji tas-sigurtà.

[17] Ara l-Opinjoni 03/2014 tad-WP29.

[18] Hu ferm stabbilit li l-"aċċess" hu parti fundamentali mid-"disponibbiltà". Ara, pereżempju, NIST SP80053rev4, li tiddefinixxi d-disponibbiltà bħala: "Ensuring timely and reliable access to and use of information", disponibbli fuq http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 tirreferi wkoll għal: "Timely, reliable access to data and information services for authorized users". Ara https://rmf.org/wpcontent/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 ukoll tiddefinixxi d-disponibbiltà bħala "Property of being accessible and usable upon demand by an authorized entity": https://www.iso.org/obp/ui/#iso:std:isoiec:27000:ed-4:v1:en

20. Tista' tqum il-kwistjoni ta' jekk telf temporanju tad-disponibbiltà ta' *data* personali għandux jitqies bħala ksur u, jekk iva, jekk dan huwiex ksur li għandu jiġi notifikat. L-Artikolu 32 tal-GDPR, "Sigurtà tal-ipproċessar", jispjega li meta jiġu implimentati miżuri tekniċi u organizzattivi biex jiġi żgurat livell ta' sigurtà xieraq għar-riskju, għandha tingħata kunsiderazzjoni, fost affarijiet oħra, għall-"*kapaċità li jiġu żgurati l-kunfidenzjalità, l-integrità, id-disponibbiltà u r-reżiljenza kontinwi tas-sistemi u s-servizzi ta' pproċessar*" u għall-"*kapaċità li jiġu restawrati d-disponibbiltà u l-aċċess għad-data personali fil-pront fil-każ ta' inċident fiżiku jew tekniku*".

21. Għaldaqstant, inċident tas-sigurtà li jirriżulta fl-indisponibbiltà ta' *data* personali għal perjodu ta' żmien ukoll hu tip ta' ksur, peress li n-nuqqas ta' aċċess għad-*data* jista' jkollu impatt sinifikanti fuq id-drittijiet u l-libertajiet tal-persuni fiżiċi. Biex kollox ikun ċar, meta d-*data* personali ma tkunx disponibbli minħabba t-twettiq ta' manutenzjoni ppjanata tas-sistema, dan ma jkunx "ksur tas-sigurtà" kif definit fl-Artikolu 4(12) tal-GDPR.

22. Bħal b'telf permanenti jew b'qerda ta' *data* personali (jew tabilħaqq kwalunkwe tip ieħor ta' ksur), ksur li jinvolvi t-telf temporanju tad-disponibbiltà għandu jkun dokumentat f'konformità mal-Artikolu 33(5) tal-GDPR. Dan jassisti lill-kontrollur biex juri r-responsabbiltà lill-awtorità superviżorja, li tista' titlob li tara dawk ir-rekords[19]. Madankollu, skont iċ-ċirkostanzi tal-ksur, jista' jew ma jistax jitlob notifika lill-awtorità superviżorja u komunikazzjoni lill-individwi affettwati. Il-kontrollur ikollu bżonn jivvaluta l-probabbiltà u s-severità tal-impatt fuq id-drittijiet u fuq il-libertajiet tal-persuni fiżiċi bħala riżultat tan-nuqqas ta' disponibbiltà ta' *data* personali. F'konformità mal-Artikolu 33 tal-GDPR, il-kontrollur ikollu bżonn jinnotifika sakemm il-ksur ma jkunx improbabbli li jirriżulta f'riskju għad-drittijiet u għal-libertajiet tal-individwi. Ovvjament, dan ikollu bżonn jiġi vvalutat fuq bażi ta' każ b'każ.

Eżempju

Fil-kuntest ta' sptar, jekk ma jkunx hemm *data* medika kritika dwar il-pazjenti disponibbli, anki b'mod temporanju, dan jista' jippreżenta riskju għad-drittijiet u għal-libertajiet tal-individwi; pereżempju jistgħu jitħassru operazzjonijiet u jinxteħtu f'riskju l-ħajjiet.

Għall-kuntrarju, fil-każ ta' sistemi ta' kumpanija medjatika li jkunu indisponibbli għal diversi sigħat (eż. minħabba qtugħ tad-dawl), jekk dik il-kumpanija mbagħad ma titħalliex tibgħat bullettini lill-abbonati tagħha, ikun improbabbli li dan jippreżenta riskju għad-drittijiet u għal-libertajiet tal-individwi.

23. Ta' min jinnota li għad li telf tad-disponibbiltà tas-sistemi ta' kontrollur jista' jkun temporanju biss u jaf ma jkollux impatt fuq l-individwi, importanti li l-kontrollur jikkunsidra l-konsegwenzi possibbli kollha ta' ksur, peress li dan xorta waħda jista' jkun jeħtieġ notifika għal raġunijiet oħra.

Eżempju

Infezzjoni b'software ta' riskatt (software malizzjuż li jikkripta d-*data* tal-kontrollur sakemm jitħallas rikatt) tista' twassal għal telf temporanju tad-disponibbiltà jekk id-*data* tista' tiġi rkuprata mill-kopji ta' riżerva. Madankollu, intrużjoni fin-network xorta waħda tkun seħħet, u tista' tkun meħtieġa notifika jekk l-inċident jiġi kwalifikat bħala ksur tal-kunfidenzjalità (jiġifieri d-*data* personali tiġi aċċessata mit-trasgressur) u dan jippreżenta riskju għad-drittijiet u għal-libertajiet tal-individwi.

3. Il-konsegwenzi possibbli ta' ksur ta' *data* personali

24. 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-

[19] Ara l-Artikolu 33(5) tal-GDPR.

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[20].

25. Għaldaqstant, il-GPDR jeħtieġ li l-kontrollur jinnotifika ksur lill-awtorità superviżorja kompetenti, sakemm ma jkunx improbabbli li dan jirriżulta f'riskju li jseħħu t-tali effetti avversi. Meta jkun hemm riskju għoli probabbli li jseħħu dawn l-effetti avversi, il-GDPR jeħtieġ li l-kontrollur jikkomunika l-ksur lill-individwi affettwati malli dan ikun raġonevolment fattibbli[21].

26. L-importanza li jkun jista' jiġi identifikat ksur, għall-valutazzjoni tar-riskju għall-individwi, u mbagħad issir notifika jekk tkun meħtieġa, hi enfasizzata fil-Premessa 87 tal-GDPR:

> "*Għandu jiġi vverifikat jekk kull protezzjoni teknoloġika xierqa u miżuri organizzattivi ġewx implimentati biex jiġi stabbilit immedjatament jekk seħħitx vjolazzjoni ta' data personali u biex jiġu informati minnufih l-awtorità superviżorja u s-suġġett tad-data. Il-fatt li n-notifika saret mingħajr dewmien żejjed għandu jiġi stabbilit filwaqt li jitqiesu b'mod partikolari n-natura u l-gravità tal-vjolazzjoni tad-data personali u l-konsegwenzi u l-effetti negattivi tagħha għas-suġġett tad-data. Notifika bħal din tista' tirriżulta f'intervent mill-awtorità superviżorja f'konformità mal-kompiti u s-setgħat tagħha stabbiliti f'dan ir-Regolament.*"

27. Linji gwida ulterjuri dwar il-valutazzjoni tar-riskju ta' effetti avversi għall-individwi huma kkunsidrati fit-Taqsima IV.

28. Jekk il-kontrolluri jonqsu milli jinnotifikaw lill-awtorità superviżorja jew inkella lis-suġġetti tad-*data* dwar ksur ta' *data* jew lit-tnejn anki jekk jiġu ssodisfati r-rekwiżiti tal-Artikoli 33 u/jew 34 tal-GDPR, l-awtorità superviżorja jkollha għażla li trid tinkludi kunsiderazzjoni tal-miżuri korrettivi kollha għad-dispożizzjoni tagħha, li jkunu jinkludu kunsiderazzjoni tal-impożizzjoni tal-multa amministrattiva xierqa[22], flimkien ma' miżura korrettiva skont l-Artikolu 58(2) tal-GDPR jew waħedha. Meta tingħażel multa amministrattiva, il-valur ta' din jista' jitla' sa €10,000,000 jew sa 2 % tal-fatturat annwali dinji totali ta' impriża skont l-Artikolu 83(4)(a) tal-GDPR. Importanti wkoll li jitfakkar li f'ċerti każijiet, in-nuqqas ta' notifika ta' ksur jista' jikxef nuqqas ta' miżuri ta' sigurtà eżistenti jew inkella inadegwatezza tal-miżuri ta' sigurtà eżistenti. Il-Linji Gwida tad-WP29 dwar il-multi amministrattivi jistipulaw: "*L-okkorrenza ta' ħafna ksur differenti li twettqu flimkien f'każ wieħed partikolari jfisser li l-awtorità superviżorja tista' tapplika l-multi amministrattivi f'livell li jkun effettiv, proporzjonat u dissważiv fil-limitu tal-aktar ksur gravi*". F'dak il-każ, l-awtorità superviżorja se jkollha wkoll il-possibbiltà li toħroġ sanzjonijiet għal nuqqas ta' notifika jew ta' komunikazzjoni tal-ksur (l-Artikoli 33 u 34 tal-GDPR) minn naħa, u nuqqas ta' miżuri (adegwati) ta' sigurtà (l-Artikolu 32 tal-GDPR) min-naħa l-oħra, peress li dawn huma żewġ tipi ta' ksur separati.

II. ARTIKOLU 33 - NOTIFIKA LILL-AWTORITÀ SUPERVIŻORJA

A. Meta tinnotifika

1. Rekwiżiti tal-Artikolu 33

29. L-Artikolu 33(1) tal-GDPR jipprovdi li:

> "*Fil-każ ta' ksur ta' data personali, il-kontrollur għandu mingħajr dewmien bla bżonn u, fejn fattibbli, mhux aktar tard minn 72 siegħa wara li jkun sar jaf bih, jinnotifika l-ksur tad-data personali lill-awtorità superviżorja kompetenti f'konformità mal-Artikolu 55 ħlief jekk il-ksur ta' data personali x'aktarx ma*

[20] Ara wkoll il-Premessi 85 u 75 tal-GDPR.

[21] Ara wkoll il-Premessa 86 tal-GDPR.

[22] Għal aktar dettalji, ara l-Linji Gwida tad-WP29 dwar l-applikazzjoni u l-iffissar ta' multi amministrattivi, disponibbli hawn: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

jirriżultax f'riskju għad-drittijiet u l-libertajiet tal-persuni fiżiċi. Fejn in-notifika lill-awtorità superviżorja ma ssirx fi żmien 72 siegħa, hija għandha tkun akkumpanjata minn raġunijiet għad-dewmien."

30. Il-Premessa 87 tal-GDPR tiddikjara[23]:

"*Għandu jiġi vverifikat jekk kull protezzjoni teknoloġika xierqa u miżuri organizzattivi ġewx implimentati biex jiġi stabbilit immedjatament jekk seħħitx vjolazzjoni ta' data personali u biex jiġu informati minnufih l-awtorità superviżorja u s-suġġett tad-data. Il-fatt li n-notifika saret mingħajr dewmien żejjed għandu jiġi stabbilit filwaqt li jitqiesu b'mod partikolari n-natura u l-gravità tal-vjolazzjoni tad-data personali u l-konsegwenzi u l-effetti negattivi tagħha għas-suġġett tad-data. Notifika bħal din tista' tirriżulta f'intervent mill-awtorità superviżorja f'konformità mal-kompiti u s-setgħat tagħha stabbiliti f'dan ir-Regolament.*"

2. Kontrollur meta "jsir jaf"?

31. Kif spjegat aktar 'il fuq, il-GDPR jeħtieġ li, f'każ ta' ksur, il-kontrollur għandu jinnotifika l-ksur mingħajr dewmien żejjed u, fejn fattibbli, mhux aktar tard minn 72 siegħa wara li jsir jaf bih. Dan jista' jqajjem il-kwistjoni ta' meta kontrollur jista' jitqies li "jsir jaf" bi ksur. L-EDPB iqis li kontrollur għandu jitqies li jkun "sar jaf" meta dak il-kontrollur ikollu livell raġonevoli ta' ċertezza li seħħ inċident tas-sigurtà li wassal biex id-*data* personali tkun kompromessa.

32. Madankollu, kif indikat qabel, il-GDPR jeħtieġ li l-kontrollur jimplimenta l-miżuri tekniċi xierqa kollha ta' protezzjoni u organizzattivi biex jistabbilixxi minnufih jekk seħħx ksur u biex jinforma minnufih lill-awtorità superviżorja u lis-suġġetti tad-*data*. Jiddikjara wkoll li l-fatt li n-notifika tkun saret mingħajr dewmien żejjed għandu jiġi stabbilit filwaqt li jitqiesu b'mod partikolari n-natura u l-gravità tal-ksur u l-konsegwenzi u l-effetti negattivi tagħha għas-suġġett tad-*data*[24]. Dan jixħet obbligu fuq il-kontrollur biex jiżgura li dan "isir jaf" bi kwalunkwe ksur fil-ħin biex ikun jista' jieħu l-azzjoni xierqa.

33. Meta, eżattament, kontrollur jista' jitqies li "sar jaf" bi ksur partikolari jkun jiddependi miċ-ċirkustanzi tal-ksur speċifiku. F'ċerti każijiet, ikun relattivament ċar mill-bidu nett li jkun seħħ ksur, filwaqt li f'oħrajn jista' jkun hemm bżonn ta' ċertu żmien biex jiġi stabbilit jekk ġietx kompromessa *data* personali. Madankollu, l-enfasi għandha tinxteħet fuq it-teħid ta' azzjoni minnufih biex jiġi investigat inċident għad-determinazzjoni ta' jekk seħħx tabilħaqq ksur tad-*data* personali, u jekk iva, biex tittieħed azzjoni rimedjali u jiġi notifikat jekk ikun hemm bżonn.

Eżempji

1. Fil-każ ta' telf ta' USB key b'*data* personali mhux kriptata, spiss ma jkunx possibbli li jiġi żgurat jekk persuni mhux awtorizzati aċċessawx dik id-*data*. Minkejja dan, għad li l-kontrollur jaf ma jkunx jista' jistabbilixxi jekk seħħx ksur tal-kunfidenzjalità, każ bħal dan irid jiġi notifikat peress li jkun hemm livell raġonevoli ta' ċertezza li seħħ ksur tad-disponibbiltà; il-kontrollur "isir jaf" meta jintebaħ li ntilfet il-USB key.

2. Parti terza tinforma lil kontrollur li aċċidentalment irċeviet id-*data* personali ta' wieħed mill-klijenti tiegħu u tipprovdi evidenza tad-divulgazzjoni mhux awtorizzata. Peress li l-kontrollur jiġi ppreżentat b'evidenza ċara ta' ksur tal-kunfidenzjalità, ma jista' jkun hemm ebda dubju li "sar jaf".

3. Kontrollur isib li seħħet intrużjoni possibbli fin-network tiegħu. Il-kontrollur jivverifika s-sistemi tiegħu biex jistabbilixxi jekk *data* personali miżmuma fuq dik is-sistema ġietx kompromessa u jikkonferma li dan hu l-każ. Mill-ġdid, peress li issa l-kontrollur ikollu evidenza ċara ta' ksur, ma jista' jkun hemm ebda dubju li "sar jaf".

[23] Il-Premessa 85 tal-GDPR hi importanti wkoll hawnhekk.

[24] Ara l-Premessa 87 tal-GDPR.

4. Ċiberkriminal jikkuntattja lill-kontrollur wara li jkun daħallu fis-sistema bla permess biex jitlob ħlas għar-riskatt. F'dak il-każ, wara li jivverifika s-sistema tiegħu biex jikkonferma li ġiet attakkata, il-kontrollur ikollu evidenza ċara li seħħ ksur u ma jkun hemm ebda dubju li sar jaf.

34. Wara li l-ewwel jiġi informat dwar ksur potenzjali minn individwu, minn organizzazzjoni medjatika, jew minn sors ieħor, jew meta hu stess jiskopri inċident tas-sigurtà, il-kontrollur jista' jagħmel perjodu qasir ta' investigazzjoni biex jistabbilixxi jekk fil-fatt seħħx ksur. Matul dan il-perjodu ta' investigazzjoni, il-kontrollur ma jistax jitqies li "sar jaf". Madankollu, hu mistenni li l-investigazzjoni inizjali tibda mill-aktar fis possibbli u tistabbilixxi b'livell raġonevoli ta' ċertezza jekk seħħx ksur; imbagħad tkun tista' ssir investigazzjoni aktar dettaljata.

35. Ladarba l-kontrollur isir jaf, ksur notifikabbli jrid jiġi notifikat mingħajr dewmien żejjed u, fejn fattibbli, mhux aktar tard minn 72 siegħa. Matul dan il-perjodu, il-kontrollur għandu jivvaluta r-riskju probabbli għall-individwi biex jiddetermina jekk ir-rekwiżit għan-notifika tnediex, kif ukoll l-azzjoni(jiet) meħtieġa biex jiġi indirizzat il-ksur. Madankollu, kontrollur jaf diġà jkollu valutazzjoni inizjali tar-riskju potenzjali li jista' jirriżulta minn ksur bħala parti minn valutazzjoni tal-impatt tal-protezzjoni tad-*data* (DPIA)[25] li ssir qabel ma titwettaq l-operazzjoni ta' proċessar ikkonċernata. Madankollu, id-DPIA tista' tkun aktar ġeneralizzata meta mqabbla maċ-ċirkustanzi speċifiċi ta' kwalunkwe ksur, u b'hekk se jkun hemm bżonn li fi kwalunkwe każ issir valutazzjoni addizzjonali li tikkunsidra dawk iċ-ċirkustanzi. Għal aktar dettalji dwar il-valutazzjoni tar-riskju, ara t-Taqsima IV.

36. F'ħafna mill-każijiet, dawn l-azzjonijiet preliminari għandhom jitwettqu ftit wara t-twissija inizjali (jiġifieri meta l-kontrollur jew il-proċessur jissuspetta li seħħ inċident tas-sigurtà li jista' jinvolvi *data* personali). – għandu jittieħed żmien itwal minn dan f'każijiet eċċezzjonali biss.

Eżempju

Individwu jinforma lill-kontrollur li rċieva ittra elettronika li tippersonifika lill-kontrollur li fiha *data* personali relatata mal-użu (propju) tiegħu tas-servizz tal-kontrollur, xi ħaġa li tissuġġerixxi li s-sigurtà tal-kontrollur ġiet kompromessa. Il-kontrollur jiddedika perjodu qasir ta' investigazzjoni u jidentifika intrużjoni fin-network tiegħu u evidenza ta' aċċess mhux awtorizzat għal *data* personali. Il-kontrollur issa jitqies li "sar jaf" u jkun hemm bżonn ta' notifika lill-awtorità superviżorja sakemm ma jkunx improbabbli li dan jippreżenta riskju għad-drittijiet u għal-libertajiet tal-individwi. Il-kontrollur se jkollu bżonn jieħu azzjoni rimedjali xierqa biex jindirizza l-ksur.

37. Għaldaqstant, il-kontrollur għandu jkollu proċessi interni fis-seħħ biex ikun jista' jindividwa u jindirizza ksur. Pereżempju, għas-sejbien ta' ċerti irregolaritajiet fil-proċessar ta' *data*, il-kontrollur jew il-proċessur jista' juża ċerti miżuri tekniċi bħal analizzaturi tal-fluss u tar-reġistrazzjoni tad-*data*, li minnhom hu possibbli li jiġu definiti avvenimenti u twissijiet bil-korrelazzjoni ta' kwalunkwe *data* tar-reġistrazzjoni[26]. Importanti li meta jiġi identifikat ksur, dan jiġi rrapportat 'il fuq lil-livell xieraq tal-maniġment biex ikun jista' jiġi indirizzat u, jekk ikun meħtieġ, notifikat f'konformità mal-Artikolu 33 u, jekk ikun hemm bżonn, mal-Artikolu 34. Miżuri u mekkaniżmi ta' rapportar bħal dawn jistgħu jiġu spjegati fil-pjanijiet ta' rispons għal inċident u/jew fl-arranġamenti ta' governanza tal-kontrollur. Dawn jgħinu lill-kontrollur jippjana b'mod effettiv u jiddetermina min għandu responsabbiltà operazzjonali fi ħdan l-organizzazzjoni għall-ġestjoni ta' ksur u kif jew jekk jeskalax inċident kif xieraq.

38. Il-kontrollur għandu jkollu fis-seħħ ukoll arranġamenti ma' kwalunkwe proċessar li juża l-kontrollur, li hu stess għandu l-obbligu li jinnotifika lill-kontrollur f'każ ta' ksur (ara aktar 'il quddiem).

[25] Ara l-Linji Gwida WP248 tad-WP29 dwar id-DPIAs hawnhekk: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[26] Ta' min jinnota li *data* tar-reġistrazzjoni li tiffaċilita l-kapaċità tal-awditjar ta', pereżempju, ħżin, modifiki jew tħassir ta' *data* wkoll tista' tikkwalifika bħala *data* personali relatata mal-persuna li tniedi l-operazzjoni rispettiva ta' proċessar.

39. Filwaqt li hi r-responsabbiltà tal-kontrolluri u tal-proċessuri li jimplimentaw miżuri xierqa biex ikunu jistgħu jipprevjenu ksur, jirreaġixxu għalih u jindirizzawh hemm xi passi prattiki li għandhom jittieħdu f'kull każ.

- L-informazzjoni li tikkonċerna l-avvenimenti kollha relatati mas-sigurtà għandha tingħadda lil persuna jew lil persuni responsabbli bil-kompitu ta' indirizzar tal-inċidenti, ta' stabbiliment tal-eżistenza ta' ksur u ta' valutazzjoni tar-riskju.
- Imbagħad għandu jiġi vvalutat ir-riskju għall-individwi minħabba ksur (probabbiltà ta' ebda riskju, ta' riskju jew ta' riskju għoli), filwaqt li jiġu informati t-taqsimiet rilevanti tal-organizzazzjoni.
- Għandha ssir notifika lill-awtorità superviżorja u potenzjalment komunikazzjoni tal-ksur lill-individwi affettwati, jekk ikun hemm bżonn.
- Fl-istess ħin, il-kontrollur għandu jaġixxi biex jikkontjeni u jirkupra l-ksur. Id-dokumentazzjoni tal-ksur għandha sseħħ matul l-iżvilupp tiegħu.

40. Għalhekk, għandu jkun ċar li hemm obbligu fuq il-kontrollur biex jaġixxi fuq kwalunkwe twissija inizjali u jistabbilixxi jekk fil-fatt seħħx ksur. Dan il-perjodu qasir jippermetti li ssir xi investigazzjoni, u biex il-kontrollur jiġbor evidenza u dettalji rilevanti oħra. Madankollu, ladarba l-kontrollur ikun stabbilixa b'livell raġonevoli ta' ċertezza li seħħ ksur, jekk jiġu ssodisfati l-kundizzjonijiet fl-Artikolu 33(1) tal-GDPR, imbagħad irid jinnotifika lill-awtorità superviżorja mingħajr dewmien żejjed u, fejn fattibbli, mhux aktar tard minn 72 siegħa[27]. Jekk kontrollur jonqos milli jaġixxi fil-ħin u jsir apparenti li seħħ ksur, dan jista' jitqies bħala nuqqas ta' notifika f'konformità mal-Artikolu 33 tal-GDPR.

41. L-Artikolu 32 tal-GDPR jagħmilha ċara li l-kontrollur u l-proċessur għandu jkollhom miżuri tekniċi u organizzattivi xierqa fis-seħħ biex jiżguraw livell xieraq ta' sigurtà tad-*data* personali: il-ħila li jiġi identifikat, indirizzat, u rapportat ksur fil-pront għandha titqies bħala elementi essenzjali ta' dawn il-miżuri.

3. Kontrolluri konġunti

42. L-Artikolu 26 tal-GDPR jikkonċerna l-kontrolluri konġunti u jispeċifika li l-kontrolluri konġunti għandhom jiddeterminaw ir-responsabbiltajiet rispettivi tagħhom għall-konformità mal-GDPR[28]. Dan se jinkludi d-determinazzjoni ta' liema parti se jkollha r-responsabbiltà biex tikkonforma mal-obbligi skont l-Artikoli 33 u 34 tal-GDPR. L-EDPB jirrakkomanda li l-arranġamenti kuntrattwali bejn il-kontrolluri konġunti jinkludu dispożizzjonijiet li jiddeterminaw liema kontrollur se jieħu r-rwol ta' mexxej jew ikun responsabbli għall-konformità mal-obbligi ta' notifika ta' ksur tal-GDPR.

4. Obbligi tal-proċessur

43. Il-kontrollur iżomm ir-responsabbiltà ġenerali għall-protezzjoni ta' *data* personali, iżda l-proċessur għandu rwol importanti x'jaqdi biex il-kontrollur ikun jista' jikkonforma mal-obbligi tiegħu; u dan jinkludi notifika ta' ksur. Tabilħaqq, l-Artikolu 28(3) tal-GDPR jispeċifika li l-ipproċessar minn proċessur għandu jkun regolat b'kuntratt jew b'att legali ieħor. L-Artikolu 28(3)(f) jiddikjara li l-kuntratt jew att legali ieħor għandu jistipula li l-proċessur "jassisti lill-kontrollur sabiex jassigura l-konformità mal-obbligi skont l-Artikoli 32 sa 36 waqt li titqies in-natura tal-ipproċessar u l-informazzjoni disponibbli lill-proċessur".

44. L-Artikolu 33(2) tal-GDPR jagħmilha ċara li jekk proċessur jintuża minn kontrollur u l-proċessur isir jaf bi ksur tad-*data* personali li jkun qed jipproċessa f'isem il-kontrollur, dan irid jinnotifika lill-kontrollur "mingħajr dewmien żejjed". Ta' min jinnota li l-proċessur ma għandux bżonn li l-ewwel jivvaluta l-probabbiltà li jiġġarrab riskju minn ksur qabel ma jinnotifika lill-kontrollur; hu l-kontrollur li jrid jagħmel

[27] Ara r-Regolament Nru 1182/71 li jistabbilixxi r-regoli applikabbli għal perjodi, dati u limiti taż-żmien, disponibbli hawn: http://eur-lex.europa.eu/legal-content/MT/TXT/HTML/?uri=CELEX:31971R1182&from=EN

[28] Ara wkoll il-Premessa 79 tal-GDPR.

din il-valutazzjoni malli jsir jaf bil-ksur. Il-proċessur irid biss jistabbilixxi jekk seħħx ksur u mbagħad jinnotifika lill-kontrollur. Il-kontrollur juża l-proċessur biex jilħaq l-għanijiet tiegħu; għaldaqstant, fil-prinċipju, il-kontrollur għandu jitqies li "sar jaf" ladarba l-proċessur jinformah bil-ksur. L-obbligu tal-proċessur li jinnotifika lill-kontrollur tiegħu jippermetti lill-kontrollur jindirizza l-ksur u jiddetermina jekk huwiex meħtieġ li jinnotifika lill-awtorità superviżorja f'konformità mal-Artikolu 33(1) u lill-individwi affettwati f'konformità mal-Artikolu 34(1). Il-kontrollur jista' wkoll ikun jixtieq jinvestiga l-ksur, peress li l-proċessur jaf ma jkunx f'pożizzjoni li jkun jaf il-fatti rilevanti kollha relatati mal-kwistjoni, pereżempju, jekk ikun għad hemm kopja jew kopja ta' riżerva ta' *data* personali meqruda jew mitlufa mill-proċessur għand il-kontrollur. Dan jista' jaffettwa jekk il-kontrollur imbagħad ikollux bżonn jinnotifika.

45. Il-GDPR ma jistipulax terminu perentorju espliċitu li sa dan il-proċessur irid iwissi lill-kontrollur, ħlief li jrid jagħmel dan "mingħajr dewmien żejjed". Għaldaqstant, l-EDPB jirrakkomanda li l-proċessur jinnotifika minnufih lill-kontrollur, b'aktar informazzjoni dwar il-ksur ipprovduta f'fażijiet aktar ma jsiru disponibbli d-dettalji. Dan hu importanti biex il-kontrollur ikun megħjun jissodisfa r-rekwiżit ta' notifika lill-awtorità superviżorja fi żmien 72 siegħa.

46. Kif spjegat aktar 'il fuq, il-kuntratt bejn il-kontrollur u l-proċessur għandu jispeċifika kif ir-rekwiżiti espressi fl-Artikolu 33(2) għandhom jiġu ssodisfati minbarra dispożizzjonijiet oħra fil-GDPR. Dan jista' jinkludi rekwiżiti għal notifika kmieni mill-proċessur li min-naħa tagħhom jappoġġjaw l-obbligi tal-kontrollur li jirrapporta lill-awtorità superviżorja fi żmien 72 siegħa.

47. Meta l-proċessur jipprovdi servizzi lil diversi kontrolluri li lkoll ikunu affettwati mill-istess inċident, il-proċessur ikollu jirrapporta d-dettalji tal-inċident lil kull kontrollur.

48. Proċessur jista' jagħmel notifika f'isem il-kontrollur, jekk il-kontrollur ikun ta lill-proċessur l-awtorizzazzjoni xierqa u dan ikun parti mill-arranġamenti kuntrattwali bejn il-kontrollur u l-proċessur. Din in-notifika trid issir f'konformità mal-Artikoli 33 u 34 tal-GDPR. Madankollu, ta' min jgħid li r-responsabbiltà legali tan-notifika tibqa' tal-kontrollur.

B. Forniment tal-informazzjoni lill-awtorità superviżorja

1. Informazzjoni li jeħtieġ tingħata

49. Meta kontrollur jinnotifika ksur lill-awtorità superviżorja, l-Artikolu 33(3) tal-GDPR jiddikjara li, tal-anqas, in-notifika għandha:

> *"(a) tiddeskrivi n-natura tal-ksur ta' data personali inklużi, fejn hu possibbli, il-kategoriji u n-numru approssimattiv tas-suġġetti tad-data kkonċernati u l-kategoriji u n-numru approssimattiv ta' data personali rreġistrata kkonċernata;*
>
> (b) *tagħti l-isem u d-dettalji tal-kuntatt tal-uffiċjal tal-protezzjoni tad-data jew ta' punt ta' kuntatt ieħor minn fejn tista' tinkiseb aktar informazzjoni;*
>
> (c) *tiddeskrivi l-konsegwenzi mistennija tal-ksur ta' data personali;*
>
> (d) *tiddeskrivi l-miżuri mittieħda jew proposti li jridu jittieħdu mill-kontrollur sabiex jindirizza l-ksur ta' data personali, inkluż, fejn xieraq, miżuri biex itaffi l-effetti ħżiena possibbli*."

50. Il-GDPR ma jiddefinix il-kategoriji ta' suġġetti tad-*data* jew tar-rekords ta' *data* personali. Madankollu, l-EDPB jissuġġerixxi kategoriji ta' suġġetti ta' *data* biex jirreferi għad-diversi tipi ta' individwi li d-*data* personali tagħhom tkun ġiet affettwata minn ksur: skont id-deskritturi użati, dawn jistgħu jinkludu, fost l-oħrajn, tfal u gruppi vulnerabbli oħra, nies b'diżabilitajiet, impjegati jew klijenti. B'mod simili, il-kategoriji ta' rekords ta' *data* personali jistgħu jirreferu għat-tipi differenti ta' rekords li l-kontrollur jista' jipproċessa, bħal *data* dwar is-saħħa, rekords dwar l-edukazzjoni, informazzjoni dwar il-bżonnijiet soċjali, dettalji finanzjarji, numri tal-kontijiet bankarji, numri tal-passaporti u l-bqija.

51. Il-Premessa 85 tal-GDPR tagħmilha ċara li wieħed mill-iskopijiet tan-notifika hu l-limitazzjoni tal-ħsara lill-individwi. Għalhekk, jekk it-tipi ta' suġġetti ta' *data* jew it-tipi ta' *data* personali jindikaw riskju ta' ħsara partikolari li sseħħ minħabba ksur (eż. serq ta' identità, frodi, telf finanzjarju, theddida għas-segretezza professjonali), importanti li n-notifika tindika dawn il-kategoriji. B'dan il-mod, din hi marbuta mar-rekwiżit ta' deskrizzjoni tal-konsegwenzi probabbli tal-ksur.

52. Meta ma jkunx hemm informazzjoni preċiża disponibbli (eż. numru eżatt ta' suġġetti ta' *data* affettwati), din ma għandhiex tkun ostaklu għal notifika ta' ksur fil-ħin. Il-GDPR jippermetti li jsiru approssimazzjonijiet fl-għadd ta' individwi affettwati u fl-għadd ta' rekords ta' *data* personali kkonċernati. L-enfasi għandha tinxteħet fuq l-indirizzar tal-effetti avversi tal-ksur minflok fuq il-forniment ta' ċifri preċiżi.

53. B'hekk, meta jkun sar ċar li seħħ ksur, iżda ma tkunx għadha magħrufa l-firxa ta' dan, notifika f'fażijiet (ara aktar 'il quddiem) hi mod sikur kif jiġu ssodisfati l-obbligi ta' notifika.

54. L-Artikolu 33(3) tal-GDPR jiddikjara li l-kontrollur għandu "mill-inqas" jipprovdi din l-informazzjoni b'notifika, biex kontrollur ikun jista', jekk ikollu bżonn, jagħżel li jipprovdi aktar dettalji. Tipi differenti ta' ksur (tal-kunfidenzjalità, tal-integrità jew tad-disponibbiltà) jistgħu jkunu jeħtieġu li tiġi pprovduta aktar informazzjoni biex jiġu spjegati b'mod sħiħ iċ-ċirkustanzi ta' kull każ.

Eżempju

Bħala parti min-notifika tiegħu lill-awtorità superviżorja, kontrollur jaf isibha utli li jsemmi l-proċessur tiegħu jekk dan ikun il-kawża ewlenija ta' ksur, b'mod partikolari jekk dan ikun wassal għal inċident li affettwa r-rekords ta' *data* personali ta' ħafna kontrolluri oħra li jużaw l-istess proċessur.

55. Fi kwalunkwe każ, l-awtorità superviżorja tista' titlob aktar dettalji bħala parti mill-investigazzjoni tagħha dwar ksur.

2. Notifika f'fażijiet

56. Skont in-natura ta' ksur, investigazzjoni ulterjuri mill-kontrollur tista' tkun meħtieġa biex jiġu stabbiliti l-fatti rilevanti kollha relatati mal-inċident. Għaldaqstant, l-Artikolu 33(4) tal-GDPR jiddikjara:

"*Fejn, u sa fejn mhuwiex possibbli li tiġi pprovduta l-informazzjoni fl-istess ħin, l-informazzjoni tista' tiġi pprovduta f'fażijiet mingħajr dewmien bla bżonn*."

57. Dan ifisser li l-GDPR jagħraf li l-kontrolluri mhux dejjem se jkollhom l-informazzjoni neċessarja kollha rigward ksur fi żmien 72 siegħa minn meta jsiru jafu bih, peress li d-dettalji sħaħ u komprensivi dwar l-inċidenti jaf mhux dejjem ikunu disponibbli f'dan il-perjodu inizjali. B'hekk, jippermetti li ssir notifika f'fażijiet. Hu aktar probabbli li dan se jkun il-każ għal ksur aktar kumpless, bħal xi tipi ta' inċidenti taċ-ċibersigurtà li fihom, pereżempju, investigazzjoni forensika approfondita tista' tkun neċessarja biex jiġu stabbiliti bis-sħiħ in-natura tal-ksur u kemm ġiet kompromessa d-*data* personali. Konsegwentement, f'ħafna każijiet il-kontrollur se jkollu jinvestiga aktar u jagħti segwitu b'informazzjoni addizzjonali f'mument aktar tard. Dan hu permissibbli, dment li l-kontrollur jipprovdi raġunijiet għad-dewmien, f'konformità mal-Artikolu 33(1) tal-GDPR. L-EDPB jirrakkomanda li meta l-kontrollur l-ewwel jinnotifika lill-awtorità superviżorja, il-kontrollur għandu jinforma wkoll lill-awtorità superviżorja jekk il-kontrollur ma jkunx għad għandu l-informazzjoni meħtieġa kollha u jipprovdi aktar dettalji aktar tard. L-awtorità superviżorja għandha taqbel dwar kif u meta għandha tiġi pprovduta informazzjoni addizzjonali. Dan ma jipprevjenix lill-kontrollur milli jipprovdi aktar informazzjoni fi kwalunkwe stadju ieħor, jekk isir jaf b'dettalji rilevanti addizzjonali dwar il-ksur li jridu jiġu pprovduti lill-awtorità superviżorja.

58. L-enfasi tar-rekwiżit ta' notifika hu li jħeġġeġ lill-kontrolluri jaġixxu minnufih fuq ksur, jikkontjenuh u, jekk possibbli, jirkupraw id-*data* personali kompromessa, u jfittxu pariri rilevanti mingħand l-awtorità superviżorja. In-notifika lill-awtorità superviżorja fi ħdan l-ewwel 72 siegħa tippermetti li l-kontrollur jiżgura li d-deċiżjonijiet dwar in-notifika jew in-nuqqas ta' notifika lill-individwi jkunu korretti.

59. Madankollu, l-iskop tan-notifika tal-awtorità superviżorja mhuwiex biss biex tinkiseb gwida dwar jekk jiġux notifikati l-individwi affettwati. F'xi każijiet ikun ovvju li, minħabba n-natura tal-ksur u s-severità tar-riskju, il-kontrollur ikollu bżonn jinnotifika lill-individwi affettwati mingħajr dewmien. Pereżempju, jekk ikun hemm theddida immedjata ta' serq tal-identità, jew jekk kategoriji speċjali ta' *data* personali[29] jiġu ddivulgati online, il-kontrollur għandu jaġixxi mingħajr dewmien żejjed biex jikkontjeni l-ksur u jikkomunikah lill-individwi kkonċernati (ara t-Taqsima III). F'ċirkustanzi eċċezzjonali, dan jista' jseħħ saħansitra qabel in-notifika tal-awtorità superviżorja. B'mod aktar ġenerali, in-notifika tal-awtorità superviżorja ma tistax isservi bħala ġustifikazzjoni għal nuqqas ta' komunikazzjoni tal-ksur lis-suġġett tad-*data* fejn tkun meħtieġa.

60. Għandu jkun ċar ukoll li wara li ssir notifika inizjali, kontrollur jista' jaġġorna lill-awtorità superviżorja jekk investigazzjoni ta' segwitu tiskopri evidenza li l-inċident tas-sigurtà kien ġie kontenut u li fil-fatt ma seħħ ebda ksur. Din l-informazzjoni mbagħad tista' tiżdied mal-informazzjoni diġà mogħtija lill-awtorità superviżorja u l-inċident jiġi reġistrat kif xieraq bħala li ma jinvolvix ksur. Ma hemm ebda penali għar-rapportar ta' inċident li fl-aħħar mill-aħħar jinstab li ma kienx ksur.

Eżempju

Kontrollur jinnotifika lill-awtorità superviżorja fi żmien 72 siegħa mid-detezzjoni ta' ksur li hu tilef USB key li fiha kopja tad-*data* personali ta' wħud mill-klijenti tiegħu. Il-USB key aktar tard tinstab arkivjata ħażin fi ħdan il-bini tal-kontrollur u tiġi rkuprata. Il-kontrollur jaġġorna lill-awtorità superviżorja u jitlob l-emendar tan-notifika.

61. Ta' min jinnota li approċċ imqassam f'fażijiet għan-notifika diġà hu l-każ skont l-obbligi eżistenti tad-Direttiva 2002/58/KE, ir-Regolament 611/2013 u inċidenti oħra awtorapportati.

3. Notifiki mdewmin

62. L-Artikolu 33(1) tal-GDPR jagħmilha ċara li meta n-notifika lill-awtorità superviżorja ma ssirx fi żmien 72 siegħa, din għandha tkun akkumpanjata minn raġunijiet għad-dewmien. Dan, flimkien mal-kunċett ta' notifika f'fażijiet, jagħraf li kontrollur jaf mhux dejjem ikun jista' jinnotifika ksur fi ħdan dak il-perjodu ta' żmien, u li notifika mdewma tista' tkun permessibbli.

63. Xenarju bħal dan jista' jseħħ meta, pereżempju, kontrollur jesperjenza ksur tal-kunfidenzjalità multiplu u simili tul perjodu qasir ta' żmien, li jaffettwa numri kbar ta' suġġetti tad-*data* bl-istess mod. Kontrollur jista' jsir konxju ta' ksur u, filwaqt li jibda l-investigazzjoni tiegħu, u qabel in-notifika, jidentifika ksur simili ulterjuri, li jkollu kawżi differenti. Skont iċ-ċirkustanzi, jista' jkun hemm bżonn xi żmien biex il-kontrollur jistabbilixxi l-firxa tal-ksur u, minflok ma jinnotifika kull ksur b'mod individwali, il-kontrollur minflok jorganizza notifika sinifikattiva li tirrappreżenta ksur multiplu simili ħafna, b'kawżi differenti possibbli. Dan jista' jwassal biex in-notifika lill-awtorità superviżorja tiġi mdewma b'aktar minn 72 siegħa wara li l-kontrollur isir jaf għall-ewwel darba b'dan il-ksur.

64. Fil-verità, kull ksur individwali hu inċident rapportabbli. Madankollu, biex jiġi evitat piż eċċessiv, il-kontrollur jista' jitħalla jissottometti notifika "raggruppata" li tirrappreżenta dan il-ksur multiplu kollu, dment li dan ikun jikkonċerna l-istess tip ta' *data* personali miksura bl-istess mod, tul perjodu relattivament qasir ta' żmien. Jekk isseħħ sensiela ta' ksur li tikkonċerna tipi differenti ta' *data* personali, miksura b'modi differenti, in-notifika għandha tipproċedi bħas-soltu, b'kull ksur jiġi rrapportat f'konformità mal-Artikolu 33.

65. Filwaqt li l-GDPR jippermetti li jsiru notifiki mdewma sa ċertu punt, dawn ma għandhomx jitqiesu bħala affarijiet li jsiru b'mod regolari. Ta' min jgħid li n-notifiki raggruppati jistgħu jsiru wkoll għal ksur multiplu simili rrapportat fi żmien 72 siegħa.

[29] Ara l-Artikolu 9 tal-GDPR.

C. Ksur transfruntier u ksur fi stabbilimenti mhux tal-UE

1. Ksur transfruntier

66. Meta jsir proċessar transfruntier[30] ta' *data* personali, ksur jista' jaffettwa lis-suġġetti tad-*data* f'aktar minn Stat Membru wieħed. L-Artikolu 33(1) tal-GDPR jagħmilha ċara li meta jseħħ ksur, il-kontrollur għandu jinnotifika lill-awtorità superviżorja kompetenti f'konformità mal-Artikolu 55 tal-GDPR[31]. L-Artikolu 55(1) tal-GDPR jgħid li:

> "*Kull awtorità superviżorja għandha tkun kompetenti biex twettaq il-kompiti assenjati lilha u l-eżerċizzju tas-setgħat ikkonferiti lilha f'konformità ma' dan ir-Regolament fit-territorju tal-Istat Membru tagħha stess.*"

67. Madankollu, l-Artikolu 56(1) tal-GDPR jistipula:

> "*Mingħajr preġudizzju għall-Artikolu 55, l-awtorità superviżorja tal-istabbiliment ewlieni jew tal-istabbiliment uniku tal-kontrollur jew il-proċessur għandha tkun kompetenti biex taġixxi bħala l-awtorità superviżorja ewlenija għall-ipproċessar transkonfinali li jsir minn dak il-kontrollur jew proċessur f'konformità mal-proċedura prevista fl-Artikolu 60.*"

68. Barra minn hekk, l-Artikolu 56(6) tal-GDPR jiddikjara:

> "*L-awtorità superviżorja ewlenija għandha tkun l-interlokutur uniku tal-kontrollur jew il-proċessur għall-ipproċessar transkonfinali li jsir minn dak il-kontrollur jew proċessur.*"

69. Dan ifisser li kull meta jseħħ ksur fil-kuntest ta' proċessar transfruntier u tkun meħtieġa notifika, il-kontrollur ikollu bżonn jinnotifika lill-awtorità superviżorja prinċipali[32]. Għaldaqstant, meta jabbozza l-pjan tiegħu ta' rispons għal ksur, kontrollur irid jagħmel valutazzjoni dwar liema awtorità superviżorja hi l-awtorità superviżorja prinċipali li se jkollu bżonn jinnotifika[33]. Dan jippermetti lill-kontrollur biex iwieġeb minnufih għal ksur u jissodisfa l-obbligi tiegħu fir-rigward tal-Artikolu 33. Għandu jkun ċar li f'każ ta' ksur li jinvolvi proċessar transfruntier, notifika trid issir lill-awtorità superviżorja prinċipali, li ma tkunx bilfors dik ta' fejn jinsabu s-suġġetti tad-*data* affettwati, jew tabilħaqq fejn seħħ il-ksur. Meta jinnotifika lill-awtorità prinċipali, il-kontrollur għandu jindika, fejn xieraq, jekk il-ksur jinvolvix stabbilimenti li jinsabu fi Stati Membri oħra, u f'liema Stati Membri s-suġġetti tad-*data* għandhom probabbiltà li jkunu affettwati mill-ksur. Jekk il-kontrollur ikollu xi dubju dwar l-identità tal-awtorità superviżorja prinċipali, tal-anqas għandu jinnotifika lill-awtorità superviżorja lokali fejn seħħ il-ksur.

2. Ksur fi stabbilimenti mhux tal-UE

70. L-Artikolu 3 tal-GDPR jikkonċerna l-kamp ta' applikazzjoni territorjali tal-GDPR, inkluż fejn japplika għall-proċessar ta' *data* personali minn kontrollur jew minn proċessur mhux stabbilit fl-UE. B'mod partikolari, l-Artikolu 3(2) tal-GDPR jiddikjara[34]:

> "*Dan ir-Regolament japplika għall-ipproċessar tad-data personali ta' suġġetti tad-data li jinsabu fl-Unjoni minn kontrollur jew proċessur mhux stabbilit fl-Unjoni, meta l-attivitajiet ta' pproċessar huma relatati ma':*

---

[30] Ara l-Artikolu 4(23) tal-GDPR.

[31] Ara wkoll il-Premessa 122 tal-GDPR.

[32] Ara l-Linji Gwida tad-WP29 għall-identifikazzjoni tal-awtorità superviżorja prinċipali ta' kontrollur jew ta' proċessur, disponibbli fuq http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[33] Lista ta' dettalji ta' kuntatt għall-awtoritajiet nazzjonali Ewropej kollha għall-protezzjoni tad-*data* tinstab hawn: https://edpb.europa.eu/about-edpb/about-edpb/members_mt

[34] Ara wkoll il-Premessi 23 u 24 tal-GDPR.

(a) *l-offerta ta' prodotti jew servizzi, irrispettivament jekk ikunx meħtieġ ħlas mis-suġġett tad-data, għal tali suġġetti tad-data fl-Unjoni; jew*

(b) *il-monitoraġġ tal-imġiba tagħhom sakemm l-imġiba tagħhom isseħħ fl-Unjoni*."

71. L-Artikolu 3(3) hu rilevanti wkoll u jiddikjara[35]:

"*Dan ir-Regolament japplika għall-ipproċessar tad-data personali minn kontrollur mhux stabbilit fl-Unjoni, iżda f'post fejn tapplika l-liġi ta' Stat Membru permezz tal-liġi internazzjonali pubblika*."

72. Għaldaqstant, meta kontrollur mhux stabbilit fl-UE jkun soġġett għall-Artikolu 3(2) jew għall-Artikolu 3(3) tal-GDPR u jesperjenza ksur, dan xorta jkun marbut bl-obbligi ta' notifika skont l-Artikoli 33 u 34 tal-GDPR. L-Artikolu 27 tal-GDPR jeħtieġ li kontrollur (u proċessur) jinnominaw rappreżentat fl-UE fejn japplika l-Artikolu 3(2) tal-GDPR.

73. Madankollu, is-sempliċi preżenza ta' rappreżentant fi Stat Membru ma tagħtix bidu għas-sistema ta' punt uniku ta' servizz[36]. Għal din ir-raġuni, jenħtieġ li l-ksur jiġi nnotifikat lil kull awtorità superviżorja li għaliha s-suġġetti tad-*data* affettwati jirrisjedu fl-Istat Membru tagħhom. Din in-notifika għandha tkun/Dawn in-notifiki għandhom ikunu r-responsabbiltà tal-kontrollur[37].

74. B'mod simili, meta proċessur ikun soġġett għall-Artikolu 3(2) tal-GDPR, dan se jkun marbut bl-obbligi fuq il-proċessuri u, ta' rilevanza partikolari hawnhekk, id-dmir li jinnotifika ksur lill-kontrollur skont l-Artikolu 33(2) tal-GDPR.

D. Kundizzjonijiet li fihom mhix meħtieġa notifika

75. L-Artikolu 33(1) tal-GDPR jagħmilha ċara li ksur "li probabbilment mhux se jirriżulta f'riskju għad-drittijiet u l-libertajiet tal-persuni fiżiċi" ma jeħtieġx notifika lill-awtorità superviżorja. Eżempju jista' jkun meta d-*data* personali diġà tkun pubblikament disponibbli u divulgazzjoni tat-tali *data* ma tkunx tikkostitwixxi riskju probabbli għall-individwu. Dan hu f'kuntrast mar-rekwiżiti eżistenti ta' notifika ta' ksur għall-fornituri ta' servizzi tal-komunikazzjoni elettronika disponibbli pubblikament fid-Direttiva 2009/136/KE li jiddikjaraw li kull ksur rilevanti jrid jiġi notifikat lill-awtorità kompetenti.

76. Fl-Opinjoni 03/2014 tiegħu dwar in-notifika ta' ksur[38], id-WP29 spjega li ksur tal-kunfidenzjalità ta' *data* personali li kienet kriptata permezz ta' algoritmu tal-ogħla livell ta' żvilupp tekniku jibqa' ksur ta' *data* personali, u jrid jiġi notifikat. Madankollu, jekk il-kunfidenzjalità tal-kjavi tibqa' intatta – jiġifieri l-kjavi ma tkunx ġiet kompromessa f'xi ksur ta' sigurtà, u tkun ġiet iġġenerata biex ma tkunx tista' tiġi aċċessata b'mezzi tekniċi disponibbli minn ebda persuna li ma tkunx awtorizzata taċċessaha – id-*data* fil-prinċipju ma tkunx intelliġibbli. B'hekk, il-ksur ikun improbabbli li affettwa b'mod avvers lill-individwi u, għaldaqstant, ma tkunx teħtieġ komunikazzjoni lil dawk l-individwi[39]. Madankollu, anki meta d-*data* tiġi kriptata, telf jew alterazzjoni jista' jkollhom konsegwenzi negattivi għas-suġġetti tad-*data* meta l-

---

[35] Ara wkoll il-Premessa 25 tal-GDPR.

[36] Ara l-Linji Gwida tad-WP29 għall-identifikazzjoni tal-awtorità superviżorja prinċipali ta' kontrollur jew ta' proċessur, disponibbli fuq http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[37] F'konformità mal-Linji Gwida 3/2018 dwar il-kamp ta' applikazzjoni territorjali tal-GDPR (l-Artikolu 3), disponibbli fuq https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_mt, l-EDPB iqis il-funzjoni ta' rappreżentant fl-Unjoni bħala mhux kompatibbli mar-rwol ta' uffiċjal estern tal-protezzjoni tad-*data* ("UPD"), u għaldaqstant ir-responsabbiltà li jinnotifika lill-awtorità superviżorja f'każ ta' ksur ta' *data* personali tibqa' dik tal-kontrollur f'konformità mal-Artikolu 27(5) tal-GDPR. Madankollu, rappreżentant jista' jkun involut fil-proċess ta' notifika jekk dan ikun ġie stipulat b'mod espliċitu fil-mandat bil-miktub.

[38] Ara l-Opinjoni 03/2014 tad-WP29 dwar in-notifika ta' ksur ta' *data* personali http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[39] Ara wkoll l-Artikolu 4(1) u (2) tar-Regolament 611/2013.

kontrollur ma jkollu ebda kopja ta' riżerva adegwata. F'dak il-każ, il-komunikazzjoni lis-suġġetti tad-*data* tkun meħtieġa, anki jekk id-data stess tkun soġġetta għal miżuri adegwati ta' kriptaġġ.

77. Id-WP29 spjega wkoll li b'mod simili dan ikun il-każ jekk id-*data* personali, bħall-passwords, ikunu ġew hashed u salted b'mod sigur, il-valur hashed ikun ġie kkalkolat b'funzjoni keyed hash kriptografika tal-ogħla livell ta' żvilupp tekniku, il-kjavi li tkun intużat għall-hash tad-*data* ma tkunx ġiet kompromessa f'ebda ksur, u l-kjavi użata għall-hashing tad-*data* tkun ġiet iġġenerata b'mod li ma tkunx tista' tiġi aċċessata b'mezzi teknoloġiċi disponibbli minn ebda persuna li mhix awtorizzata taċċessaha.

78. Konsegwentement, jekk id-*data* personali tkun saret essenzjalment mhux intelliġibbli għal partijiet mhux awtorizzati u meta d-*data* tkun kopja jew tkun teżisti kopja ta' riżerva, ksur tal-kunfidenzjalità li jinvolvi *data* personali kriptata kif xieraq jaf ma jkollux bżonn jiġi notifikat lill-awtorità superviżorja. Dan għaliex ksur bħal dan ma jkollux probabbiltà li jippreżenta riskju għad-drittijiet u għal-libertajiet tal-individwi. Ovvjament dan ifisser li l-individwu lanqas ma jkollu bżonn jiġi informat peress li aktarx li ma jkun hemm ebda riskju għoli. Madankollu, ta' min ifakkar li filwaqt li n-notifika inizjalment jaf ma tkunx meħtieġa jekk ma jkun hemm ebda riskju probabbli għad-drittijiet u għal-libertajiet tal-individwi, dan jista' jinbidel maż-żmien u r-riskju jkollu bżonn jerġa' jiġi evalwat. Pereżempju, jekk eventwalment jinstab li l-kjavi hi kompromessa, jew tinkixef vulnerabbiltà fis-software kriptografiku, in-notifika xorta jaf tkun meħtieġa.

79. Barra minn hekk, ta' min jinnota li jekk iseħħ ksur u ma jkun hemm ebda kopja ta' riżerva tad-*data* personali kriptata, ikun seħħ ksur tad-disponibbiltà, li jista' jġib miegħu riskji għall-individwi u, għalhekk, jista' jkun jeħtieġ notifika. B'mod simili, meta jseħħ ksur li jinvolvi t-telf ta' *data* kriptata, anki jekk tkun teżisti kopja ta' riżerva tad-*data* personali, dan xorta jista' jkun ksur rapportabbli, skont it-tul ta' żmien meħud għar-restawr tad-*data* minn dik il-kopja ta' riżerva u l-effett li jkollu n-nuqqas ta' disponibbiltà fuq l-individwi. Kif jiddikjara l-Artikolu 32(1)(c) tal-GDPR, fattur importanti tas-sigurtà hu l-"*kapaċità li jiġu restawrati d-disponibbiltà u l-aċċess għad-data personali fil-pront fil-każ ta' inċident fiżiku jew tekniku*".

Eżempju

Ksur li ma jkunx jeħtieġ notifika lill-awtorità superviżorja jkun it-telf ta' apparat mobbli kriptat b'mod sigur, użat mill-kontrollur u mill-persunal tiegħu. Dment li l-kjavi kriptografika tibqa' fil-pussess sigur tal-kontrollur u din ma tkunx l-unika kopja tad-*data* personali, id-*data* personali tkun inaċċessibbli għal trasgressur. Dan ifisser li jkun improbabbli li l-ksur jirriżulta f'riskju għad-drittijiet u għal-libertajiet tal-individwi tas-suġġetti tad-*data* inkwisjtoni. Jekk aktar tard isir evidenti li l-kjavi kriptografika ġiet kompromessa jew li s-software kriptografiku jew l-algoritmu huma vulnerabbli, ir-riskju għad-drittijiet u għal-libertajiet tal-individwi jinbidel u b'hekk issa jaf ikun hemm bżonn ta' notifika.

80. Madankollu, nuqqas ta' konformità mal-Artikolu 33 tal-GDPR jeżisti meta kontrollur ma jinnotifikax lill-awtorità superviżorja f'sitwazzjoni li fiha d-*data* fil-fatt ma tkunx ġiet kriptata b'mod sigur. Għaldaqstant, meta jagħżlu s-software kriptografiku, il-kontrolluri għandhom joqogħdu ferm attenti li jiżnu l-kwalità u l-implimentazzjoni xierqa tal-kriptaġġ offrut, jifhmu x'livell ta' protezzjoni fil-fatt jipprovdi u jekk huwiex adattat għar-riskji ppreżentati. Il-kontrolluri għandhom ikunu midħla wkoll tad-dettalji ta' kif jaħdem il-prodott kriptografiku tagħhom. Pereżempju, apparat jista' jiġi kriptat ladarba jintefa, iżda mhux meta jkun f'modalità stand-by. Uħud mill-prodotti li jużaw kriptaġġ għandhom "kjavi predefiniti" li jridu jinbidlu minn kull klijent biex ikunu effettivi. Il-kriptaġġ jista' jiġi kkunsidrat adegwat minn esperti tas-sigurtà f'mument partikolari, iżda jaf isir skadut wara ftit snin, li jfisser li ma jkunx ċert jekk id-*data* hix kriptata biżżejjed minn dak il-prodott u li dan jipprovdi livell xieraq ta' protezzjoni.

III. ARTIKOLU 34 – KOMUNIKAZZJONI LIS-SUĠĠETT TAD-*DATA*

A. Individwi informati

81. F'ċerti każijiet, minbarra li jinnotifika lill-awtorità superviżorja, il-kontrollur ikun meħtieġ jikkomunika ksur lill-individwi affettwati wkoll.

L-Artikolu 34(1) tal-GDPR jiddikjara:

> "*Meta l-ksur ta' data personali probabbilment ikun se jirriżulta f'riskju għoli għad-drittijiet u l-libertajiet tal-persuni fiżiċi l-kontrollur għandu jikkomunika l-ksur ta' data personali lis-suġġett tad-data mingħajr dewmien bla bżonn*."

82. Il-kontrolluri għandhom ifakkru li n-notifika lill-awtorità superviżorja hi obbligatorja sakemm ma jkunx improbabbli li jkun hemm riskju għad-drittijiet u għal-libertajiet tal-individwi bħala riżultat ta' ksur. Barra minn hekk, meta jkun hemm probabbiltà ta' riskju għoli għad-drittijiet u għal-libertajiet tal-individwi minħabba ksur, l-individwi jridu jiġu informati wkoll. Għaldaqstant, il-livell limitu għall-komunikazzjoni ta' ksur lill-individwi hu ogħla minn dak għan-notifika tal-awtoritajiet superviżorji u, għaldaqstant, mhux kull ksur se jkollu bżonn jiġi komunikat lill-individwi, u b'hekk ikunu protetti minn għeja li jġibu magħhom notifiki żejda.

83. Il-GDPR jiddikjara li l-komunikazzjoni ta' ksur lill-individwi għandha ssir "mingħajr dewmien bla bżonn", li jfisser mill-aktar fis possibbli. L-objettiv ewlieni tan-notifika lill-individwi hu li tiġi pprovduta informazzjoni speċifika dwar il-passi li għandhom jieħdu biex jipproteġu lilhom infushom[40]. Kif innotat aktar 'il fuq, skont in-natura tal-ksur u r-riskju miġjub, komunikazzjoni fil-ħin tgħin lill-individwi jieħdu passi biex jipproteġu lilhom infushom minn kwalunkwe konsegwenza negattiva tal-ksur.

84. L-Anness B ta' dawn il-Linji Gwida jipprovdi lista mhux eżawrjenti ta' eżempji ta' meta ksur jaf ikollu probabbiltà li jirriżulta f'riskju għoli għall-individwi u, konsegwentement, każijiet li fihom kontrollur ikollu jinnotifika ksur lil dawk affettwati.

B. Informazzjoni li jeħtieġ tingħata

85. Meta jiġu notifikati l-individwi, l-Artikolu 34(2) tal-GDPR jispeċifika li:

> "*Il-komunikazzjoni lis-suġġett tad-data msemmija fil-paragrafu 1 ta' dan l-Artikolu għandha tiddeskrivi b'lingwaġġ ċar u sempliċi n-natura tal-ksur ta' data personali u tinkludi mill-inqas l-informazzjoni u l-miżuri imsemmija fil-punti (b), (c) u (d) tal-Artikolu 33(3)*."

86. Skont din id-dispożizzjoni, il-kontrollur tal-anqas għandu jipprovdi l-informazzjoni li ġejja:

- deskrizzjoni tan-natura tal-ksur;
- l-isem u d-dettalji ta' kuntatt tal-uffiċjal tal-protezzjoni tad-*data* jew ta' punt ta' kuntatt ieħor;
- deskrizzjoni tal-konsegwenzi probabbli tal-ksur; u
- deskrizzjoni tal-miżuri meħuda jew proposti li jridu jittieħdu mill-kontrollur biex jindirizza l-ksur, inklużi, fejn xieraq, miżuri li jtaffu l-effetti avversi possibbli tiegħu.

87. Bħala eżempju tal-miżuri meħuda għall-indirizzar tal-ksur u għall-mitigazzjoni tal-effetti avversi possibbli tiegħu, il-kontrollur jista' jiddikjara li, wara li jinnotifika l-ksur lill-awtorità superviżorja rilevanti, il-kontrollur irċieva parir dwar il-ġestjoni tal-ksur u t-tnaqqis tal-impatt tiegħu. Fejn xieraq, il-kontrollur għandu jipprovdi wkoll pariri speċifiċi lill-individwi biex jipproteġu lilhom infushom kontra l-konsegwenzi avversi possibbli tal-ksur, bħar-risettjar tal-passwords f'każ li jkunu ġew kompromessi l-

[40] Ara wkoll il-Premessa 86 tal-GDPR.

kredenzjali tal-aċċess tagħhom. Mill-ġdid, kontrollur jista' jagħżel li jipprovdi aktar informazzjoni minn dik li hi meħtieġa hawnhekk.

C. Ikkuntattjar tal-individwi

88. Fil-prinċipju, il-ksur rilevanti għandu jiġi komunikat lis-suġġetti tad-*data* affettwati b'mod dirett, sakemm dan ma jkunx jinvolvi sforz sproporzjonat. F'każ bħal dan, minflok għandu jkun hemm komunikazzjoni pubblika jew miżura simili fejn is-suġġetti tad-*data* jiġu informati b'mod għaldaqstant effettiv (l-Artikolu 34(3)(c) tal-GDPR).

89. Għandhom jintużaw messaġġi dedikati meta ksur jiġi komunikat lis-suġġetti tad-*data* u dawn ma għandhomx jintbagħtu ma' informazzjoni oħra, bħal aġġornamenti regolari, bullettini jew messaġġi standard. Dan jgħin biex il-komunikazzjoni tal-ksur tkun ċara u trasparenti.

90. Eżempji ta' metodi ta' komunikazzjoni trasparenti jinkludu messaġġi diretti (eż. ittra elettronika, SMS, messaġġ dirett), kartelluni jew notifika fuq siti web prominenti, komunikazzjonijiet postali u reklami prominenti fil-midja stampata. Notifika ristretta biss fi ħdan stqarrija għall-istampa jew fi blogg korporattiv ma tkunx mezz effettiv ta' komunikazzjoni ta' ksur lil individwu. L-EDPB jirrakkomanda li l-kontrolluri għandhom jużaw mezz li jimmassimizza l-probabbiltà ta' komunikazzjoni xierqa tal-informazzjoni lill-individwi affettwati kollha. Skont iċ-ċirkustanzi, dan jista' jfisser li l-kontrollur iħaddem diversi metodi ta' komunikazzjoni, minflok ma juża mezz wieħed ta' kuntatt.

91. Il-kontrolluri jaf ikollhom bżonn jiżguraw ukoll li l-komunikazzjoni tkun aċċessibbli f'formati alternattivi xierqa u f'lingwi rilevanti biex jiżguraw li l-individwi jkunu jistgħu jifhmu l-informazzjoni li tiġi pprovduta lilhom. Pereżempju, meta jikkomunikaw ksur lil individwu, ġeneralment ikun xieraq li mar-riċevitur tintuża l-lingwa użata matul il-perkors normali preċedenti tan-negozju. Madankollu, jekk il-ksur jaffettwa s-suġġetti tad-*data* li l-kontrollur ma jkunx interaġixxa magħhom preċedentement, jew b'mod partikolari dawk li jirresjedu fi Stat Membru differenti jew f'pajjiż ieħor mhux tal-UE fejn hu stabbilit il-kontrollur, il-komunikazzjoni fil-lingwa nazzjonali lokali tista' tkun aċċettabbli, b'kunsiderazzjoni tar-riżorsa meħtieġa. L-aktar ħaġa importanti hi li s-suġġetti tad-*data* jiġu megħjuna jifhmu n-natura tal-ksur u l-passi li jistgħu jieħdu biex jipproteġu lilhom infushom.

92. Il-kontrolluri jinsabu fl-aħjar pożizzjoni biex jiddeterminaw l-aktar mezz ta' kuntatt xieraq biex jikkomunikaw ksur lill-individwi, partikolarment jekk dawn jinteraġixxu mal-klijenti tagħhom fuq bażi frekwenti. Madankollu, hu ċar li kontrollur għandu joqgħod attent jekk juża mezz ta' kuntatt kompromess mill-ksur peress li dan il-mezz jista' jintuża wkoll mit-trasgressuri li jimpersonaw lill-kontrollur.

93. Fl-istess ħin, il-Premessa 86 tal-GDPR tispjega li:

> "*Tali komunikazzjonijiet lis-suġġetti tad-data għandhom jsiru 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 oħra, 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*."

94. Għaldaqstant, il-kontrolluri jaf ikunu jixtiequ jikkuntattjaw u jikkonsultaw lill-awtorità superviżorja mhux biss biex jiksbu pariri dwar l-informar lis-suġġetti tad-*data* dwar ksur f'konformità mal-Artikolu 34, iżda anki dwar il-messaġġi xierqa li għandhom jintbagħtu lill-individwi, u l-aktar mezz xieraq biex jikkuntattjaw lil dawn.

95. B'rabta ma' dan hemm il-parir mogħti fil-Premessa 88 tal-GDPR li n-notifika ta' ksur għandha tikkunsidra "l-interessi leġittimi tal-awtoritajiet tal-infurzar tal-liġi fejn l-iżvelar bikri jista' jxekkel mingħajr bżonn l-investigazzjoni taċ-ċirkostanzi ta' vjolazzjoni ta' *data* personali". Dan jista' jfisser li f'ċerti ċirkustanzi, fejn ġustifikat, u skont il-parir tal-awtoritajiet ta' infurzar tal-liġi, il-kontrollur jista'

jittardja l-komunikazzjoni tal-ksur lill-individwi affettwati sakemm jasal żmien tali li ma jkunux preġudikati t-tali investigazzjonijiet. Madankollu, is-suġġetti tad-*data* xorta jkunu jridu jiġu informati kif xieraq wara dan iż-żmien.

96. Kull meta ma jkunx possibbli għall-kontrollur li jikkomunika ksur lil individwu għaliex ikun hemm *data* insuffiċjenti maħżuna biex jiġi kkuntattjat l-individwu, f'dik iċ-ċirkustanza partikolari l-kontrollur għandu jinforma lill-individwu malli jkun raġonevolment fattibbli li jagħmel dan (eż. meta individwu jeżerċita d-dritt tiegħu skont l-Artikolu 15 biex jaċċessa d-*data* personali u jipprovdi lill-kontrollur bl-informazzjoni addizzjonali neċessarja biex jikkuntattjah).

D. Kundizzjonijiet li fihom mhix meħtieġa komunikazzjoni

97. L-Artikolu 34(3) tal-GDPR jiddikjara tliet kundizzjonijiet li, jekk jiġu ssodisfati, ma tkunx meħtieġa n-notifika lill-individwi fil-każ ta' ksur. Dawn huma:

    - Il-kontrollur ikun applika miżuri tekniċi u organizzazzjonali xierqa biex jipproteġi d-*data* personali qabel il-ksur, b'mod partikolari dawk il-miżuri li jrendu d-*data* personali mhux intelliġibbli għal kwalunkwe persuna li ma tkunx awtorizzata taċċessaha. Dawn jistgħu jinkludu, pereżempju, il-protezzjoni ta' *data* personali bi kriptaġġ tal-ogħla livell ta' żvilupp tekniku, jew b'tokenizzazzjoni.
    - Eżatt wara ksur, il-kontrollur ikun ħa passi biex jiżgura li r-riskju għoli miġjub għad-drittijiet u għal-libertajiet tal-individwi ma jkunx għadu probabbli li jimmaterjalizza. Pereżempju, skont iċ-ċirkustanzi tal-każ, il-kontrollur jaf ikun identifika minnufih u ħa azzjoni kontra l-individwu li jkun aċċessa d-*data* personali qabel ma dan seta' jagħmel xi ħaġa biha. Xorta trid tingħata kunsiderazzjoni xierqa lill-konsegwenzi possibbli ta' kwalunkwe ksur tal-kunfidenzjalità, mill-ġdid, skont in-natura tad-*data* kkonċernata.
    - Ikun jinvolvi sforz sproporzjonat[41] biex jiġu kkuntattjati l-individwi, forsi meta d-dettalji ta' kuntatt tagħhom ikunu ntilfu bħala riżultat tal-ksur jew ma jkunux magħrufa minn qabel. Pereżempju, il-maħżen ta' uffiċċju statistiku jegħreq u d-dokumenti li fihom id-*data* personali kienu maħżuna biss f'forma stampata. Minflok, il-kontrollur irid jagħmel komunikazzjoni pubblika jew jieħu miżura simili, li biha l-individwi jiġu informati b'mod ugwalment effettiv. Fil-każ ta' sforz sproporzjonat, jistgħu jkunu previsti wkoll arranġamenti tekniċi biex l-informazzjoni dwar il-ksur tkun disponibbli meta tintalab, li tista' tkun siewja għal dawk l-individwi li jaf ikunu ġew affettwati minn ksur, iżda l-kontrollur ma jkunx jista' jikkuntattjahom b'xi mod ieħor.

98. F'konformità mal-prinċipju ta' responsabbiltà, il-kontrolluri għandhom ikunu kapaċi juru lill-awtorità superviżorja li huma jissodisfaw waħda minn dawn il-kundizzjonijiet jew aktar[42]. Ta' min ifakkar li filwaqt li n-notifika inizjalment jaf ma tkunx meħtieġa jekk ma jkun hemm ebda riskju għad-drittijiet u għal-libertajiet tal-persuni fiżiċi, dan jista' jinbidel maż-żmien u r-riskju jkollu bżonn jerġa' jiġi evalwat.

99. Jekk kontrollur jiddeċiedi li ma jikkomunikax ksur lill-individwu, l-Artikolu 34(4) tal-GDPR jispjega li l-awtorità superviżorja tista' titolbu jagħmel dan, jekk hi tqis li l-ksur aktarx li jirriżulta f'riskju għoli għall-individwi. Inkella, din tista' tqis li l-kundizzjonijiet fl-Artikolu 34(3) tal-GDPR ġew issodisfati, f'liema każ in-notifika lill-individwi ma tkunx meħtieġa. Jekk l-awtorità superviżorja tiddetermina li d-deċiżjoni ta' nuqqas ta' notifika lis-suġġetti tad-*data* ma għandhiex bażi valida, tista' tikkunsidra li tħaddem is-setgħat u s-sanzjonijiet disponibbli tagħha.

---

[41] Ara l-Linji Gwida tad-WP29 dwar it-trasparenza, li jikkunsidraw il-kwistjoni ta' sforz sproporzjonat, disponibbli fuq http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[42] Ara l-Artikolu 5(2) tal-GDPR.

IV. VALUTAZZJONI TAR-RISKJU U TAR-RISKJU GĦOLI

A. Riskju bħala skattatur għal notifika

100. Għalkemm il-GDPR jintroduċi l-obbligu ta' notifika ta' ksur, mhuwiex rekwiżit li jrid isir f'kull ċirkustanza:

- Notifika lill-awtorità superviżorja kompetenti tkun meħtieġa sakemm ma jkunx improbabbli li ksur jirriżulta f'riskju għad-drittijiet u għal-libertajiet tal-individwi.
- Komunikazzjoni ta' ksur lill-individwu tiskatta biss fejn ikun hemm probabbiltà li dan jirriżulta f'riskju għoli għad-drittijiet u għal-libertajiet tiegħu.

101. Dan ifisser li eżatt malli jsir jaf bi ksur, hu ta' importanza vitali li l-kontrollur mhux biss ifittex li jikkontjeni l-inċident iżda jivvaluta wkoll ir-riskju li jista' jirriżulta minnu. Hemm żewġ raġunijiet importanti għal dan: l-ewwel nett, l-għarfien tal-probabbiltà u tas-severità potenzjali tal-impatt fuq l-individwu jgħin lill-kontrollur jieħu passi effettivi biex jikkontjeni u jindirizza l-ksur; it-tieni, jgħinu jiddetermina jekk hix meħtieġa n-notifika lill-awtorità superviżorja u, jekk ikun hemm bżonn, lill-individwi kkonċernati.

102. Kif spjegat aktar 'il fuq, notifika ta' ksur tkun meħtieġa sakemm ma jkunx improbabbli li dan jirriżulta f'riskju għad-drittijiet u għal-libertajiet tal-individwi, u l-iskattatur prinċipali li jeħtieġ komunikazzjoni ta' ksur lis-suġġetti tad-*data* hu meta jkun probabbli li dan jirriżulta f'riskju *għoli* għad-drittijiet u għal-libertajiet tal-individwi. Dan ir-riskju jeżisti meta l-ksur ikun jista' jwassal għal dannu fiżiku, materjali jew mhux materjali għall-individwi li d-*data* tagħhom tkun inkisret. Eżempji ta' dannu bħal dan huma diskriminazzjoni, serq jew frodi tal-identità, telf finanzjarju u ħsara għar-reputazzjoni. Meta l-ksur ikun jinvolvi *data* personali li tikxef oriġini razzjali jew etnika, opinjoni politika, twemmin reliġjuż jew filosofiku, jew sħubija fi trade union, jew tinkludi *data* ġenetika, *data* li tikkonċerna s-saħħa jew *data* li tikkonċerna l-ħajja sesswali, jew kundanni kriminali u reati jew miżuri relatati tas-sigurtà, it-tali ħsara għandha titqies li aktarx li sseħħ[43].

B. Fatturi li għandhom jiġu kkunsidrati meta jiġi vvalutat riskju

103. Il-Premessi 75 u 76 tal-GDPR jissuġġerixxu li ġeneralment, meta jiġi vvalutat riskju, għandha tingħata kunsiderazzjoni kemm lill-probabbiltà kif ukoll lis-severità tar-riskju għad-drittijiet u għal-libertajiet tas-suġġetti tad-*data*. Fih hu ddikjarat ukoll li r-riskju għandu jiġi evalwat fuq il-bażi ta' valutazzjoni oġġettiva.

104. Ta' min jinnota li l-valutazzjoni tar-riskju għad-drittijiet u għal-libertajiet tal-persuni bħala riżultat ta' ksur għandha enfasi differenti mir-riskju kkunsidrat f'DPIA)[44]. Id-DPIA tikkunsidra kemm ir-riskji tal-ipproċessar tad-*data* mwettaq kif ippjanat, kif ukoll ir-riskji f'każ ta' ksur. Meta jiġi kkunsidrat ksur potenzjali, din tħares f'termini ġenerali lejn il-probabbiltà li dan iseħħ, u l-ħsara għas-suġġetti tad-*data* li tista' ssegwi; fi kliem ieħor, hi valutazzjoni ta' avveniment ipotetiku. Bi ksur propju, l-avveniment diġà jkun seħħ, u b'hekk l-enfasi tinxteħet kollha kemm hi fuq ir-riskju li jirriżulta tal-impatt tal-ksur fuq l-individwi.

Eżempju

DPIA tissuġġerixxi li l-użu propost ta' prodott ta' software tas-sigurtà partikolari għall-protezzjoni ta' *data* personali hu miżura xierqa biex jiġi żgurat livell ta' sigurtà xieraq għar-riskju li l-ipproċessar ikun jippreżenta għall-individwi. Madankollu, jekk wara ssir magħrufa vulnerabbiltà, din tkun tbiddel l-

[43] Ara l-Premessa 75 u l-Premessa 85 tal-GDPR.

[44] Ara l-Linji Gwida tad-WP dwar id-DPIAs hawnhekk: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

idoneità tas-software għall-konteniment tar-riskju għad-*data* personali protetta u b'hekk ikun hemm bżonn li jerġa' jiġi vvalutat bħala parti minn DPIA kurrenti. Vulnerabbiltà fil-prodott tiġi sfruttata aktar tard u jseħħ ksur. Il-kontrollur għandu jivvaluta ċ-ċirkustanzi speċifiċi tal-ksur, id-*data* affettwata, u l-livell potenzjali tal-impatt fuq l-individwi, kif ukoll kemm hu probabbli li r-riskju jimmaterjalizza.

105. Għalhekk, meta jivvaluta r-riskju għall-individwi bħala riżultat ta' ksur, il-kontrollur għandu jikkunsidra ċ-ċirkustanzi speċifiċi tal-ksur, inkluża s-severità tal-impatt potenzjali u l-probabbiltà li dan iseħħ. Għaldaqstant, l-EDPB jirrakkomanda li l-valutazzjoni għandha tqis il-kriterji li ġejjin[45]:

- **It-tip ta' ksur**

106. It-tip ta' ksur li seħħ jista' jaffettwa l-livell ta' riskju ppreżentat lill-individwi. Pereżempju, ksur tal-kunfidenzjalità li fih tiġi ddivulgata informazzjoni medika lil partijiet mhux awtorizzati jista' jkollu sett differenti ta' konsegwenzi għal individwu meta mqabbel ma' ksur li fih jintilfu d-dettalji mediċi ta' individwu, u ma jibqgħux disponibbli aktar.

- **In-natura, is-sensittività u l-volum tad-*data* personali**

107. Ovvjament, meta jiġi vvalutat ir-riskju, fattur importanti hu t-tip u s-sensittività tad-*data* personali li tkun ġiet kompromessa mill-ksur. Normalment, aktar ma tkun sensittiva d-*data*, aktar ikun għoli r-riskju ta' dannu għan-nies affettwati, iżda għandha tingħata wkoll kunsiderazzjoni għal *data* personali oħra li tista' diġà tkun disponibbli dwar is-suġġett tad-*data*. Pereżempju, hu improbabbli li d-divulgazzjoni tal-isem u tal-indirizz ta' individwu f'ċirkustanzi ordinarji tikkawża dannu sostanzjali. Madankollu, jekk l-isem u l-indirizz ta' ġenitur adottiv jiġu ddivulgati lil ġenitur tat-twelid, il-konsegwenzi jistgħu jkunu serji ħafna kemm għall-ġenitur adottiv kif ukoll għall-minorenni.

108. Kull ksur li jinvolvi *data* dwar is-saħħa, dokumenti tal-identità, jew *data* finanzjarja bħal dettalji ta' karti tal-kreditu, jista' jikkawża dannu waħdu, iżda jekk jitħallat mal-oħrajn jista' jintuża għal serq tal-identità. *Data* personali mħallta tipikament tkun aktar sensittiva minn biċċa waħda ta' *data* personali.

109. Ċerti tipi ta' *data* personali jaf għall-ewwel jidhru pjuttost innokwi, madankollu, dak li d-*data* jaf tikxef dwar l-individwu affettwat għandu jiġi kkunsidrat bir-reqqa. Lista ta' klijenti li jaċċettaw konsenji regolari jaf ma tkunx partikolarment sensittiva, iżda l-istess *data* dwar klijenti li talbu li l-konsenji tagħhom jitwaqqfu waqt li jkunu fuq btala tkun informazzjoni siewja għall-kriminali.

110. B'mod simili, ammont żgħir ta' *data* personali ferm sensittiva jista' jkollu impatt qawwi fuq individwu, u firxa kbira ta' dettalji tista' tikxef firxa akbar ta' informazzjoni dwar dak l-individwu. Barra minn hekk, ksur li jaffettwa volumi kbar ta' *data* personali dwar ħafna suġġetti tad-*data* jista' jkollu effett fuq għadd korrispondenti kbir ta' individwi.

- **Faċilità ta' identifikazzjoni tal-individwi**

111. Fattur importanti x'jiġi kkunsidrat hu kemm se jkun faċli biex parti li jkollha aċċess għal *data* personali kompromessa tidentifika individwi speċifiċi, jew tqabbel id-*data* ma' informazzjoni oħra biex tidentifika lill-individwi. Skont iċ-ċirkustanzi, l-identifikazzjoni tista' tkun possibbli direttament mid-*data* personali miksura b'ebda riċerka speċjali meħtieġa biex tiġi skopruta l-identità tal-individwu, jew jista' jkun estremament diffiċli li titqabbel id-*data* personali ma' individwu partikolari, iżda dan xorta jista' jkun għadu possibbli f'ċerti kundizzjonijiet. L-identifikazzjoni tista' tkun direttament jew indirettament possibbli mid-*data* miksura, iżda tista' tiddependi wkoll mill-kuntest speċifiku tal-ksur, u

[45] L-Artikolu 3.2 tar-Regolament 611/2013 jipprovdi gwida dwar il-fatturi li għandhom jiġu kkunsidrati b'rabta man-notifika ta' ksur fis-settur tas-servizzi tal-komunikazzjoni elettronika, li tista' tkun siewja fil-kuntest ta' notifika skont il-GDPR. Ara http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:mt:PDF

mid-disponibbiltà pubblika tad-dettalji personali relatati. Din tista' tkun aktar rilevanti għal ksur tal-kunfidenzjalità u tad-disponibbiltà.

112. Kif iddikjarat aktar 'il fuq, *data* personali protetta b'livell xieraq ta' kriptaġġ ma tkunx intelliġibbli għal persuni mhux awtorizzati mingħajr kjavi dekriptografika. Barra minn hekk, psewdonomizzazzjoni implimentata kif xieraq (definita fl-Artikolu 4(5) tal-GDPR bħala "*l-ipproċessar ta' data personali b'tali mod li d-data personali ma tkunx tista' tibqa' tiġi attribwita għal suġġett tad-data speċifiku mingħajr l-użu ta' informazzjoni addizzjonali, dment li tali informazzjoni addizzjonali tinżamm separatament u tkun soġġetta għal miżuri tekniċi u organizzattivi biex jiġi żgurat li d-data personali ma tiġix attribwita għal persuna fiżika identifikata jew identifikabbli*") ukoll tista' tnaqqas il-probabbiltà li individwi jiġu identifikati f'każ ta' ksur. Madankollu, tekniki ta' psewdonimizzazzjoni waħedhom ma jistgħux jitqiesu li jagħmlu d-*data* mhux intelliġibbli.

- **Severità tal-konsegwenzi għall-individwi**

113. Skont in-natura tad-*data* personali involuta fi ksur, pereżempju, kategoriji speċjali ta' *data*, id-dannu potenzjali għall-individwi li jista' jirriżulta jista' tkun partikolarment sever, b'mod partikolari meta l-ksur ikun jista' jirriżulta f'serq jew fi frodi tal-identità, fi ħsara fiżika, fi tbatija psikoloġika, f'umiljazzjoni jew fi ħsara għar-reputazzjoni. Jekk il-ksur jikkonċerna *data* personali dwar individwi vulnerabbli, dawn jistgħu jitqiegħdu f'riskju akbar ta' ħsara.

114. Jekk il-kontrollur ikunx jaf li d-*data* personali tinsab f'idejn persuni li l-intenzjonijiet tagħhom mhumiex magħrufa jew potenzjalment huma malizzjużi jista' jkollu impatt fuq il-livell ta' riskju potenzjali. Jista' jkun hemm ksur tal-kunfidenzjalità, li fih id-*data* personali tiġi ddivulgata lil parti terza, kif definita fl-Artikolu 4(10), jew lil riċevitur ieħor bi żball. Dan jista' jseħħ, pereżempju, meta d-*data* personali tintbagħat bi żball lid-dipartiment żbaljat ta' organizzazzjoni, jew lil organizzazzjoni fornitriċi użata ta' spiss. Il-kontrollur jista' jitlob lir-riċevitur biex jibgħat lura jew inkella jeqred b'mod sigur id-*data* li rċieva. Fiż-żewġ każijiet, peress li l-kontrollur ikollu relazzjoni kurrenti mar-riċevitur, u dan jista' jkun jaf bil-proċeduri u bl-istorja tiegħu u b'dettalji rilevanti oħra, ir-riċevitur jista' jitqies "fdat". Fi kliem ieħor, il-kontrollur jista' jkollu livell ta' aċċertament mar-riċevitur biex ikun jista' jistenna b'mod raġonevoli li dik il-parti mhix se taqra jew taċċessa d-*data* mibgħuta bi żball, u li din se tikkonforma mal-istruzzjonijiet li tirritornaha. Anki jekk id-*data* tkun ġiet aċċessata, xorta waħda jkun possibbli li l-kontrollur jafda lir-riċevitur biex ma jieħu ebda azzjoni ulterjuri biha u jirritorna d-*data* lill-kontrollur minnufih u jikkoopera mal-irkupru tagħha. F'każijiet bħal dawn, dan jista' jiġi inkluż fil-valutazzjoni tar-riskju li l-kontrollur jagħmel wara l-ksur – il-fatt li r-riċevitur hu fdat jista' jxejjen is-severità tal-konsegwenzi tal-ksur iżda dan ma jfissirx li ma seħħx ksur. Madankollu, min-naħa tiegħu dan jista' jneħħi l-probabbiltà ta' riskju għall-individwi, u b'hekk ma jkunx jeħtieġ aktar in-notifika lill-awtorità superviżorja, jew lill-individwi affettwati. Mill-ġdid, dan jiddependi minn valutazzjoni fuq bażi ta' każ b'każ. Minkejja dan, il-kontrollur xorta waħda jrid iżomm l-informazzjoni li tikkonċerna l-ksur bħala parti mid-dmir ġenerali li jżomm rekords dwar il-ksur (ara t-Taqsima V aktar 'il quddiem).

115. Għandha tingħata kunsiderazzjoni lill-permanenza tal-konsegwenzi għall-individwi, fejn l-impatt jista' jitqies li jkun akbar jekk l-effetti jkunu fit-tul.

- **Karatteristiki speċjali tal-individwu**

116. Ksur jista' jaffettwa d-*data* personali li tikkonċerna lit-tfal jew lil individwi vulnerabbli oħra, li jistgħu jkunu f'riskju akbar ta' periklu b'riżultat ta' dan. Jista' jkun hemm fatturi oħra dwar l-individwu li jistgħu jaffettwaw il-livell tal-impatt tal-ksur fuqu.

- **Karatteristiki speċjali tal-kontrollur tad-*data***

117. In-natura u r-rwol tal-kontrollur u tal-attivitajiet tiegħu jistgħu jaffettwaw ir-riskju għall-individwu b'riżultat ta' ksur. Pereżempju, organizzazzjoni medika tipproċessa kategoriji speċjali ta' *data* personali, li jfisser li hemm theddida akbar għall-individwi jekk id-*data* personali tagħhom tinkiser, meta mqabbla ma' lista ta' indirizzi tal-konsenja ta' gazzetta.

- **L-għadd ta' individwi affettwati**

118. Ksur jista' jaffettwa individwu wieħed biss jew ftit individwi jew diversi eluf, jekk mhux ħafna aktar. Ġeneralment, aktar ma jkun kbir l-għadd ta' individwi affettwati, aktar ikun kbir l-impatt li jista' jkollu ksur. Madankollu, ksur jista' jkollu impatt sever anki fuq individwu wieħed, skont in-natura tad-*data* personali u l-kuntest li fih tkun ġiet kompromessa. Mill-ġdid, hu importanti li jiġu kkunsidrati l-probabbiltà u s-severità tal-impatt fuq dawk affettwati.

- **Punti ġenerali**

119. Għaldaqstant, meta jivvaluta r-riskju li aktarx li jirriżulta minn ksur, il-kontrollur għandu jikkunsidra taħlita tas-severità tal-impatt potenzjali fuq id-drittijiet u fuq il-libertajiet tal-individwi u tal-probabbiltà li dawn iseħħu. Jidher ċar li, meta l-konsegwenzi ta' ksur ikunu aktar severi, ir-riskju jkun akbar u, b'mod simili, meta l-probabbiltà li dawn iseħħu tkun akbar, anki r-riskju jkun ogħla. Jekk jiġi f'dubju, il-kontrollur għandu jiżbalja fuq in-naħa tal-kawtela u jinnotifika. L-Anness B jipprovdi xi eżempji siewja ta' tipi differenti ta' ksur li jinvolvu riskju jew riskju għoli għall-individwi.

120. L-Aġenzija tal-Unjoni Ewropea dwar is-Sigurtà tan-Networks u l-Informazzjoni (ENISA) ipproduċiet rakkomandazzjonijiet għal metodoloġija ta' valutazzjoni tas-severità ta' ksur, li l-kontrolluri u l-proċessuri jafu jsibu utli meta jfasslu l-pjan tagħhom ta' rispons għall-ġestjoni ta' ksur[46].

V. RESPONSABBILTÀ U ŻAMMA TA' REKORDS

A. Dokumentazzjoni tal-ksur

121. Indipendentement minn jekk ksur iridx jiġi notifikat lill-awtorità superviżorja, il-kontrollur irid iżomm dokumentazzjoni ta' kull ksur, kif jispjega l-Artikolu 33(5) tal-GDPR:

> "*Il-kontrollur għandu jiddokumenta kwalunkwe ksur ta' data personali, inklużi l-fatti relattivi għall-ksur tad-data personali, l-effetti tiegħu u l-azzjoni ta' rimedju meħuda. Dik id-dokumentazzjoni għandha tippermetti lill-awtorità superviżorja tivverifika l-konformità ma' dan l-Artikolu*."

122. Dan hu marbut mal-prinċipju ta' responsabbiltà tal-GDPR, li jinsab fl-Artikolu 5(2) tal-GDPR. L-iskop tar-reġistrazzjoni ta' ksur mhux notifikabbli, kif ukoll ta' ksur notifikabbli, hu marbut ukoll mal-obbligi tal-kontrollur skont l-Artikolu 24 tal-GDPR, u l-awtorità superviżorja tista' titlob li tara dawn ir-rekords. Għaldaqstant, il-kontrolluri huma mħeġġa jistabbilixxu reġistru intern ta' ksur, indipendentement minn jekk humiex meħtieġa jinnotifikaw jew le[47].

123. Filwaqt li hu f'idejn il-kontrollur li jiddetermina x'metodu u xi struttura għandhom jintużaw meta jiddokumenta ksur, f'termini ta' informazzjoni reġistrabbli hemm elementi importanti li għandhom jiġu inklużi fil-każijiet kollha. Kif inhu meħtieġ mill-Artikolu 33(5) tal-GDPR, il-kontrollur għandu bżonn jirreġistra d-dettalji li jikkonċernaw il-ksur, li għandhom jinkludu l-kawżi tiegħu, x'seħħ u d-*data* personali affettwata. Għandu jinkludi wkoll l-effetti u l-konsegwenzi tal-ksur, flimkien mal-azzjoni korrettiva meħuda mill-kontrollur.

124. Il-GDPR ma jispeċifikax perjodu ta' żamma għat-tali dokumentazzjoni. Meta t-tali rekords ikun fihom *data* personali, ikun f'idejn il-kontrollur li jiddetermina l-perjodu xieraq ta' żamma f'konformità

[46] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity

[47] Il-kontrollur jista' jagħżel li jiddokumenta ksur bħala parti mir-rekord tiegħu tal-attivitajiet ta' proċessar li jinżamm skont l-Artikolu 30 tal-GDPR. Mhuwiex meħtieġ reġistru separat, dment li l-informazzjoni rilevanti għall-ksur tkun identifikabbli b'mod ċar bħala tali u tkun tista' tiġi estratta meta tintalab.

mal-prinċipji b'rabta mal-proċessar ta' *data* personali[48] u li jissodisfa bażi legali għall-ipproċessar[49]. Ikollu bżonn iżomm id-dokumentazzjoni f'konformità mal-Artikolu 33(5) tal-GDPR peress li jista' jintalab jipprovdi evidenza tal-konformità ma' dak l-Artikolu, jew mal-prinċipju ta' responsabbiltà b'mod aktar ġenerali, lill-awtorità superviżorja. Hu ċar li, jekk ir-rekords infushom ma jkun fihom ebda *data* personali, mela l-prinċipju ta' limitazzjoni tal-ħażna[50] tal-GDPR ma japplikax.

125. Minbarra dawn id-dettalji, l-EDPB jirrakkomanda li l-kontrollur jiddokumenta wkoll il-motivazzjonijiet tiegħu għad-deċiżjonijiet meħuda bħala tweġiba għal ksur. B'mod partikolari, jekk ksur ma jiġix notifikat, għandha tiġi dokumentata ġustifikazzjoni għal dik id-deċiżjoni. Din għandha tinkludi raġunijiet dwar għaliex il-kontrollur iqis li hu improbabbli li l-ksur jirriżulta f'riskju għad-drittijiet u għal-libertajiet tal-individwi[51]. Inkella, jekk il-kontrollur iqis li ġiet issodisfata xi waħda mill-kundizzjonijiet fl-Artikolu 34(3) tal-GDPR, għandu jkun kapaċi jipprovdi l-evidenza xierqa li turi li dan hu l-każ.

126. Meta l-kontrollur jinnotifika ksur lill-awtorità superviżorja, iżda n-notifika tiġi mdewma, il-kontrollur irid ikun kapaċi jipprovdi raġunijiet għal dak id-dewmien; dokumentazzjoni relatata ma' dan tista' tgħin biex jintwera li d-dewmien fir-rapportar hu ġustifikat u mhuwiex eċċessiv.

127. Meta l-kontrollur jikkomunika ksur lill-individwi affettwati, dan għandu jkun trasparenti dwar il-ksur u jikkomunika b'mod effettiv u fil-ħin. Għalhekk, ikun ta' għajnuna li l-kontrollur juri responsabbiltà u konformità billi jżomm evidenza tat-tali komunikazzjoni.

128. Biex jgħin fil-konformità mal-Artikoli 33 u 34 tal-GDPR, ikun ta' vantaġġ kemm għall-kontrolluri kif ukoll għall-proċessuri li jkollhom proċedura dokumentata ta' notifika fis-seħħ, li tistabbilixxi l-proċess li għandu jiġi segwit ladarba jiġi individwat ksur, inkluż kif jiġi kontenut, ġestit u rkuprat l-inċident, kif ukoll li tivvaluta r-riskju, u tinnotifika l-ksur. F'dan ir-rigward, biex tintwera l-konformità mal-GDPR, jista' jkun siewi wkoll li jintwera li l-impjegati ġew informati dwar l-eżistenza tat-tali proċeduri u mekkaniżmi u li dawn jafu kif jirreaġixxu għal ksur.

129. Ta' min jinnota li nuqqas ta' dokumentazzjoni xierqa ta' ksur jista' jwassal biex l-awtorità superviżorja teżerċita s-setgħat tagħha skont l-Artikolu 58 tal-GDPR u/jew timponi multa amministrattiva f'konformità mal-Artikolu 83 tal-GDPR.

B. Rwol tal-Uffiċjal tal-Protezzjoni tad-*Data*

130. Kontrollur jew proċessur jista' jkollu Uffiċjal tal-Protezzjoni tad-*Data* (UPD)[52], kif meħtieġ mill-Artikolu 37 tal-GDPR jew inkella b'mod volontarju bħala kwistjoni ta' prattika tajba. L-Artikolu 39 tal-GDPR jistabbilixxi numru ta' kompiti obbligatorji għall-UPD, iżda ma jipprevjenix lill-kontrollur milli jalloka kompiti oħra, jekk dawn ikunu xierqa.

131. Ta' rilevanza partikolari għan-notifika ta' ksur, il-kompiti obbligatorji tal-UPD jinkludu, fost dmirijiet oħra, l-għoti ta' pariri u ta' informazzjoni dwar il-protezzjoni tad-*data* lill-kontrollur jew lill-proċessur, il-monitoraġġ tal-konformità mal-GDPR, u l-għoti ta' pariri b'rabta mad-DPIAs. L-UPD irid jikkoopera wkoll mal-awtorità superviżorja u jaġixxi bħala punt ta' kuntatt għall-awtorità superviżorja u għas-suġġetti tad-*data*. Ta' min jinnota wkoll li, meta jiġi notifikat il-ksur lill-awtorità superviżorja, l-Artikolu 33(3)(b) tal-GDPR jeħtieġ li l-kontrollur jipprovdi l-isem u d-dettalji ta' kuntatt tal-UPD tiegħu, jew ta' punt ta' kuntatt ieħor.

---

[48] Ara l-Artikolu 5 tal-GDPR.

[49] Ara l-Artikolu 6 kif ukoll l-Artikolu 9 tal-GDPR.

[50] Ara l-Artikolu 5(1)(e) tal-GDPR.

[51] Ara l-Premessa 85 tal-GDPR.

[52] Ara l-Linji Gwida tad-WP dwar l-UPD hawnhekk: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

132. F'termini tad-dokumentazzjoni tal-ksur, il-kontrollur jew il-proċessur jaf ikun jixtieq jikseb l-opinjoni tal-UPD tiegħu rigward l-istruttura, il-kompożizzjoni u l-amministrazzjoni ta' din id-dokumentazzjoni. L-UPD jista' jingħata wkoll il-kompitu addizzjonali li jżomm it-tali rekords.

133. Dawn il-fatturi jfissru li l-UPD għandu jaqdi rwol importanti fil-valutazzjoni tal-prevenzjoni ta' ksur, jew ta' tħejjija għal dan, billi jipprovdi pariri u jissorvelja l-konformità, kif ukoll matul ksur (jiġifieri meta jinnotifika lill-awtorità superviżorja), u matul kwalunkwe investigazzjoni sussegwenti mill-awtorità superviżorja. F'dan il-kuntest, l-EDPB jirrakkomanda li l-UPD jiġi informat minnufih dwar l-eżistenza ta' ksur u li jkun involut matul il-proċess kollu ta' ġestjoni u ta' notifika tal-ksur.

VI. OBBLIGI TA' NOTIFIKA SKONT STRUMENTI LEGALI OĦRA

134. Minbarra n-notifika u l-komunikazzjoni tal-ksur skont il-GDPR, u b'mod separat minn dawn, il-kontrolluri għandhom ikunu konxji wkoll dwar kwalunkwe rekwiżit li jinnotifikaw inċidenti tas-sigurtà skont leġiżlazzjoni assoċjata oħra li tista' tapplika għalihom u jekk din tistax teħtieġhom ukoll jinnotifikaw lill-awtorità superviżorja dwar ksur ta' *data* personali fl-istess ħin. Rekwiżiti bħal dawn jistgħu jvarjaw bejn l-Istati Membri, iżda eżempji ta' rekwiżiti ta' notifika fi strumenti legali oħra, u kif dawn jirrelataw mal-GDPR jinkludu dawn li ġejjin:

- *Ir-Regolament (UE) 910/2014 dwar l-identifikazzjoni elettronika u s-servizzi fiduċjarji għal tranżazzjonijiet elettroniċi fis-suq intern (ir-Regolament eIDAS)*[53].

135. L-Artikolu 19(2) tar-Regolament eIDAS jeħtieġ li l-fornituri ta' servizzi fiduċjarji jinnotifikaw lill-korp superviżorju tagħhom dwar ksur tas-sigurtà jew telf tal-integrità li jkollu impatt sinifikanti fuq is-servizz fiduċjarju pprovdut jew fuq id-*data* personali miżmuma fih. Fejn applikabbli—jiġifieri fejn it-tali ksur jew telf ikun ukoll ksur ta' *data* personali skont il-GDPR—il-fornitur ta' servizzi fiduċjarji għandu jinnotifika lill-awtorità superviżorja wkoll.

- *Id-Direttiva (UE) 2016/1148 dwar miżuri għal livell għoli komuni ta' sigurtà tan-networks u tas-sistemi tal-informazzjoni madwar l-Unjoni (id-Direttiva NIS)*[54].

136. L-Artikoli 14 u 16 tad-Direttiva NIS jeħtieġu li l-operaturi ta' servizzi essenzjali u l-fornituri ta' servizzi diġitali jinnotifikaw l-inċidenti tas-sigurtà lill-awtorità kompetenti tagħhom. Kif rikonoxxut mill-Premessa 63 tad-Direttiva NIS[55], l-inċidenti tas-sigurtà spiss jaf ikunu jinkludu kompromess ta' *data* personali. Filwaqt li d-Direttiva NIS teħtieġ li l-awtoritajiet kompetenti u l-awtoritajiet superviżorji jikkooperaw u jiskambjaw informazzjoni f'dak il-kuntest, jibqa' l-każ li meta t-tali inċidenti jkunu, jew isiru, ksur ta' *data* personali skont il-GDPR, dawk l-operaturi u/jew il-fornituri jkunu meħtieġa jinnotifikaw lill-awtorità superviżorja b'mod separat mir-rekwiżiti ta' notifika tal-inċidenti tad-Direttiva NIS.

Eżempju

Fornitur ta' servizzi ta' cloud li jinnotifika ksur skont id-Direttiva NIS jaf ikollu bżonn jinnotifika lil kontrollur ukoll, jekk dan ikun jinkludi ksur ta' *data* personali. B'mod simili, fornitur ta' servizzi fiduċjarji li jinnotifika skont ir-Regolament eIDAS jaf ikun meħtieġ jinnotifika lill-awtorità għall-protezzjoni tad-*data* rilevanti wkoll fil-każ ta' ksur.

[53] Ara http://eur-lex.europa.eu/legal-content/MT/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[54] Ara http://eur-lex.europa.eu/legal-content/MT/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

[55] Il-Premessa 63: *"Id-data personali f'bosta każijiet hija kompromessa minħabba dawn l-inċidenti. F'dan il-kuntest, l-awtoritajiet kompetenti u l-awtoritajiet għall-protezzjoni tad-data għandhom jikkooperaw u jkollhom skambju tal-informazzjoni dwar il-kwistjonijiet rilevanti kollha biex tiġi ttrattata kwalunkwe vjolazzjoni fir-rigward tad-data personali li jirriżultaw minn inċidenti."*

- *Id-Direttiva 2009/136/KE (id-Direttiva dwar id-Drittijiet taċ-Ċittadini) u r-Regolament 611/2013 (ir-Regolament dwar in-Notifika ta' Ksur).*

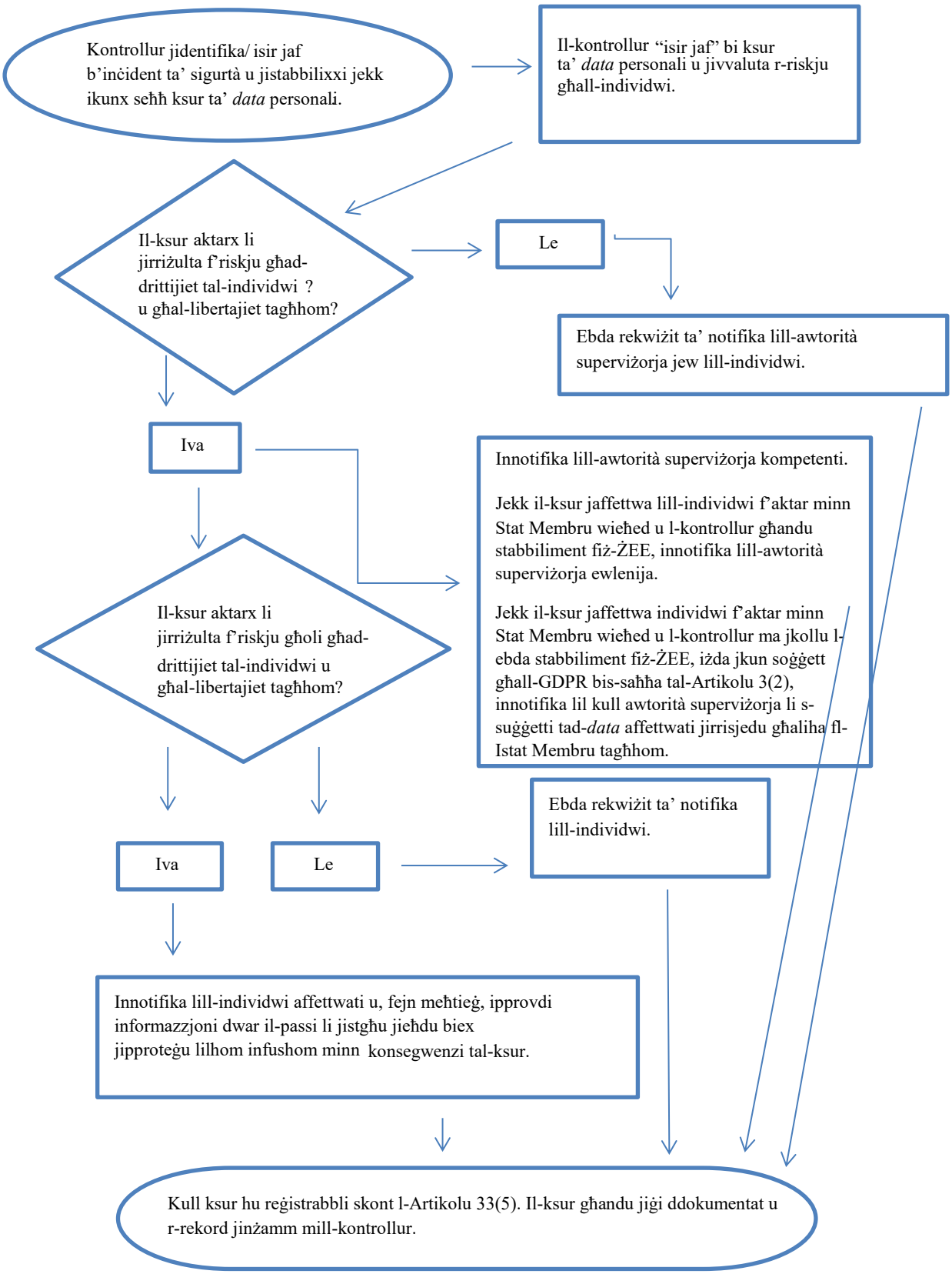
137. Il-fornituri ta' servizzi tal-komunikazzjoni elettronika disponibbli pubblikament fil-kuntest tad-Direttiva 2002/58/KE[56] jridu jinnotifikaw il-ksur lill-awtoritajiet nazzjonali kompetenti.

138. Il-kontrolluri għandhom ikunu konxji wkoll minn kwalunkwe dmir ta' notifika legali, medika, jew professjonali addizzjonali skont reġimi applikabbli oħra.

[56] Fl-10 ta' Jannar 2017, il-Kummissjoni Ewropea pproponiet Regolament dwar il-Privatezza u l-Komunikazzjonijiet Elettroniċi li se jissostitwixxi d-Direttiva 2009/136/KE u jneħħi r-rekwiżiti ta' notifika. Madankollu, sakemm il-Parlament Ewropew japprova din il-proposta jibqa' fis-seħħ ir-rekwiżit ta' notifika eżistenti, ara https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electroniccommunications

VII. ANNESS

A. Dijagramma sekwenzjali li turi r-rekwiżiti ta' notifika



B. Eżempji ta' ksur ta' *data* personali u min għandu jiġi notifikat

L-eżempji mhux eżawrjenti li ġejjin se jgħinu lill-kontrolluri biex jiddeterminaw jekk għandhomx bżonn jinnotifikaw f'xenarji differenti ta' ksur ta' *data* personali. Dawn l-eżempji jistgħu jgħinu wkoll biex issir distinzjoni bejn riskju u riskju għoli għad-drittijiet u għal-libertajiet tal-individwi.

	Eżempju	Innotifika lill-awtorità superviżorja	Innotifika lis-suġġett tad-*data*	Noti/rakkomandazzjonijiet
i	Kontrollur ħażen kopja ta' riżerva ta' arkivju ta' *data* personali kriptata fuq USB key. Il-kjavi tinsteraq waqt serqa.	Le.	Le.	Dment li d-*data* tkun kriptata b'algoritmu tal-ogħla livell ta' żvilupp tekniku, jeżistu kopji ta' riżerva tad-*data*, il-kjavi unika mhix kompromessa, u d-*data* tista' tiġi restawrata mingħajr wisq dewmien, dan jaf ma jkunx ksur rapportabbli. Madankollu, jekk aktar tard tiġi kompromessa, tkun meħtieġa notifika.
ii	Kontrollur iżomm servizz online. B'riżultat ta' ċiberattakk fuq dak is-servizz, id-*data* personali tal-individwi tiġi esfiltrata. Il-kontrollur għandu klijenti fi Stat Membru wieħed.	Iva, irrapporta lill-awtorità superviżorja jekk ikun hemm konsegwenzi probabbli għall-individwi.	Iva, irrapporta lill-individwi skont in-natura tad-*data* personali affettwata u jekk is-severità tal-konsegwenzi probabbli għall-individwi hi għolja.	
iii	Qtugħ tad-dawl qasir li jdum diversi minuti fiċ-ċentru telefoniku ta' kontrollur li jfisser li l-klijenti ma jistgħux iċemplu lill-kontrollur u jaċċessaw ir-rekords tagħhom.	Le.	Le.	Dan mhuwiex ksur notifikabbli, iżda xorta inċident reġistrabbli skont l-Artikolu 33(5). Il-kontrollur għandu jżomm rekords xierqa.
iv	Kontrollur iġarrab attakk b'software ta' riskatt li jwassal biex id-*data* kollha tiġi kriptata. Ma jkun hemm ebda kopja ta' riżerva disponibbli u d-*data* ma tkunx tista' tiġi restawrata. Matul l-investigazzjoni	Iva, irrapporta lill-awtorità superviżorja, jekk ikun hemm konsegwenzi probabbli għall-individwi peress li dan hu telf tad-disponibbiltà.	Iva, irrapporta lill-individwi, skont in-natura tad-*data* personali affettwata u l-effett possibbli tan-nuqqas ta' disponibbiltà tad-*data*, kif ukoll konsegwenzi probabbli oħra.	Jekk kien hemm kopja ta' riżerva disponibbli u d-*data* tista' tiġi restawrata mingħajr wisq dewmien, ma jkunx hemm bżonn li dan jiġi rapportat lill-awtorità superviżorja jew lill-individwi peress li ma jkun hemm ebda telf permanenti tad-disponibbiltà jew tal-kunfidenzjalità. Madankollu,

	jidher ċar li l-unika funzjonalità tas-software ta' riskatt kienet li jikkripta d-*data*, u li ma kien hemm ebda programm malizzjuż ieħor preżenti fis-sistema.			jekk l-awtorità superviżorja tkun saret taf bl-inċident b'mezz ieħor, tista' tikkunsidra investigazzjoni biex tivvaluta l-konformità mar-rekwiżiti aktar ġenerali dwar is-sigurtà tal-Artikolu 32.

v	Individwu jċempel liċ-ċentru telefoniku ta' bank biex jirrapporta ksur ta' *data*. L-individwu rċieva rendikont ta' kull xahar destinat għal xi ħadd ieħor. Il-kontrollur jagħmel investigazzjoni qasira (jiġifieri li titlesta f'24 siegħa) u jistabbilixxi b'kunfidenza raġonevoli li seħħ ksur ta' *data* personali u jekk għandux problema sistemika li tkun tfisser li hemm individwi oħra li huma affettwati jew li jistgħu jkunu affettwati.	Iva.	L-individwi affettwati biss jiġu notifikati jekk ikun hemm riskju għoli u jkun ċar li ma kienx hemm oħrajn li ġew affettwati.	Jekk, wara investigazzjoni ulterjuri, jiġi identifikat li hemm aktar individwi affettwati, irid jintbagħat aġġornament lill-awtorità superviżorja u l-kontrollur jieħu l-passi addizzjonali li jinnotifika lil individwi oħra jekk ikun hemm riskju għoli għalihom.
vi	Kontrollur jopera suq online u għandu klijenti f'diversi Stati Membri. Is-suq iġarrab ċiberattakk u l-ismijiet tal-utenti, il-passwords u r-rekords tax-xirjiet jiġu ppubblikati online mill-aggressur.	Iva, irrapporta lill-awtorità superviżorja prinċipali jekk ikun involut proċessar transfruntier.	Iva, peress li dan jista' jwassal għal riskju għoli.	Il-kontrollur għandu jieħu azzjoni, eż. billi jinforza risettjar tal-passwords fuq il-kontijiet affettwati, kif ukoll passi oħra biex jimmitiga r-riskju. Il-kontrollur għandu jikkunsidra wkoll kull obbligu ta' notifika ieħor, eż. skont id-Direttiva NIS bħala fornitur ta' servizzi diġitali.
vii	Kumpanija ta' hosting ta' siti web li taġixxi bħala proċessur tad-*data* tidentifika żball fil-kodiċi li jikkontrolla l-awtorizzazzjoni tal-utenti. L-effett tal-	Bħala l-proċessur, il-kumpanija li tospita s-sit web trid tinnotifika lill-klijenti affettwati tiegħu (il-kontrolluri) mingħajr dewmien żejjed.	Jekk aktarx li ma jkun hemm ebda riskju għoli għall-individwi, dawn ma għandhomx bżonn jiġu notifikati.	Il-kumpanija ta' hosting ta' siti web (il-proċessur) trid tikkunsidra kwalunkwe obbligu ta' notifika ieħor (eż. skont id-Direttiva NIS bħala fornitur ta' servizzi diġitali).

	iżball ifisser li kwalunkwe utent jista' jaċċessa d-dettalji tal-kont ta' kwalunkwe utent ieħor.	Jekk jiġi supponut li l-kumpanija ta' hosting ta' siti web tkun għamlet l-investigazzjoni tagħha stess, il-kontrolluri affettwati għandhom ikunu kunfidenti b'mod raġonevoli dwar jekk kull wieħed minnhom ġarrabx ksur u, għaldaqstant, aktarx li jitqiesu li "saru jafu" ladarba jiġu notifikati mill-kumpanija ta' hosting (il-proċessur). Imbagħad il-kontrollur irid jinnotifika lill-awtorità superviżorja.		Jekk ma jkun hemm ebda evidenza li din il-vulnerabbiltà tkun ġiet sfruttata minn xi wieħed mill-kontrolluri tagħha, jaf ma jkunx seħħ ksur notifikabbli iżda hu probabbli li dan ikun reġistrabbli jew ikun kwistjoni ta' nuqqas ta' konformità skont l-Artikolu 32.
viii	Ir-rekords mediċi fi sptar ma jkunux disponibbli għal perjodu ta' 30 siegħa minħabba ċiberattakk.	Iva, l-isptar hu obbligat jinnotifika peress li jista' jseħħ riskju għoli għall-benessri u għall-privatezza tal-pazjent.	Iva, irrapporta lill-individwi affettwati.	
ix	*Data* personali ta' għadd kbir ta' studenti tintbagħat bi żball lil lista ta' indirizzi żbaljata b'aktar minn 1,000 riċevitur.	Iva, irrapporta lill-awtorità superviżorja.	Iva, irrapporta lill-individwi skont l-ambitu u t-tip ta' *data* personali involuta u s-severità tal-konsegwenzi possibbli.	
x	Ittra elettronika ta' kummerċjalizzazzjoni diretta tintbagħat lir-riċevituri fil-kampi "lil:" jew "cc:", biex b'hekk kull riċevitur ikun jista' jara l-indirizz elettroniku ta' riċevituri oħra.	Iva, in-notifika lill-awtorità superviżorja jaf tkun obbligatorja jekk ikunu affettwati ħafna individwi, jekk tinkixef *data* sensittiva (eż. lista ta' indirizzi ta' psikoterapist) jew jekk hemm fatturi oħra li jippreżentaw riskji għoljin (eż. l-ittra fiha l-passwords inizjali).	Iva, irrapporta lill-individwi skont l-ambitu u t-tip ta' *data* personali involuta u s-severità tal-konsegwenzi possibbli.	In-notifika jaf ma tkunx meħtieġa jekk ma tinkixef ebda *data* sensittiva jew jekk jinkixef għadd żgħir biss ta' indirizzi elettroniċi.