



5 KORAKOV ZA VARNO UPRAVLJANJE Z DOKUMENTACIJO

Varnost podatkov je za različne deležnike različno pomembna. Ko govorimo o varnosti osebnih podatkov, gre za varnostni interes posameznika, na katerega se osebni podatek nanaša, ko govorimo o varnosti poslovnih podatkov, gre za varnostni interes organizacije in ko govorimo o varnosti tajnih podatkov, gre za varnostni interes države. V dinamičnem poslovnem okolju se največkrat srečujejo vsi trije omenjeni deležniki, torej posameznik, organizacija in država in tako prihaja do prepletanja teh treh interesov na različnih nivojih, v različnih procesih in v različnih okoljih. In v takem dinamičnem okolju ima varnost podatkov še toliko večji pomen.

Se še spomnite, ko smo kot otroci v vrtcu ali prvih razredih osnovne šole risali in pisali na tako imenovani »šmirpapir«, že uporabljen, potiskan, popisan papir, za drugotno rabo. Veliko je bilo primerov, ko smo domov staršem vsi ponosni in vzhičeni prinesli na eni strani svoje risarske izdelke, na drugi strani pa izpis plače iz nekega podjetja. Verjamem, da je to v tem času, ob povprečni stopnji varnostne ozaveščenosti, skorajda nemogoče ponovljiv scenarij, se pa sedaj pojavljajo povsem nova tveganja, povezana z upravljanjem in obdelavo raznih vrst podatkov, predvsem tistih, ki se obdelujejo v e-obliki. S

pojavom digitalizacije, digitalne transformacije poslovnih procesov podjetij in družbe kot celote, ta tveganja postajajo še bolj kompleksna in globalno izpostavljena. Naj omenim le nekaj odmevnih primerov iz zadnjega časa: vdor v Facebook račune v mesecu novembru 2018 (kompromitiranih 50 mio uporabniških računov), vdor v bazo podatkov hotelske verige Marriot (kraja podatkov 500 mio gostov potekala več let), Kršitev varstva osebnih podatkov v portugalski bolnišnici (dostop do podatkov o bolnikih – 400.000 EUR globe), kršitev varstva osebnih podatkov na letališču Heathrow Airport (zaradi slabega varstva osebnih

podatkov globa 120.000 GBF), vdor v baze osebnih podatkov zdravstvene zavarovalnice Anthem (vdor v bazo podatkov in dostop do podatkov 80 mio ljudi). Omenjene slabe prakse nakazujejo na občutljivost predvsem elektronskih baz podatkov in kompleksnost zagotavljanja dostopnosti in varnosti le-teh.

Vsa ta nova tveganja, ki se pojavljajo v digitalnem svetu, v povezavi s tveganji upravljanja z dokumentacijo v fizični obliki, nakazujejo na nujnost poznavanja in razumevanja življenjskega cikla določenega podatka in pomembnost prepoznavanja ranljivosti, ogroženosti in tveganj, ki se pojavljajo v posamezni fazi življenjskega cikla konkretnega podatka. Izkušnje in slabe prakse v zadnjem času nakazujejo predvsem na pomanjkanje zavedanja o pomenu varnosti podatkov, ki se nahajajo na različnih podatkovnih nosilcih (dokumentacija v fizični obliki, diski, CD-ji, spominski ključki ipd.) predvsem v zadnjih fazah njihovega življenjskega cikla, to je v času shranjevanja v arhivih, ko govorimo o fizični dokumentaciji in strežnikih ali prenosnih medijih, ko govorimo o dokumentaciji v e-obliki. Podjetja veliko pozornosti posvečajo upravljanju in obdelavi podatkov

Vsa ta nova tveganja, ki se pojavljajo v digitalnem svetu, v povezavi s tveganji upravljanja z dokumentacijo v fizični obliki, nakazujejo na nujnost poznavanja in razumevanja življenjskega cikla določenega podatka in pomembnost prepoznavanja ranljivosti, ogroženosti in tveganj, ki se pojavljajo v posamezni fazi življenjskega cikla konkretnega podatka.

v času, ko so le ti aktivni, torej v fazi od njihovega nastanka ali prejema, pa vse do konca njegove uporabe. In v tej fazi se v večini primerov aktivna obdelava podatka – dokumenta zaključijo. Dokument se izloči iz uporabe in na tak ali drugačen način odloži v hrambo. Obdelovalec podatka pa s tem ne zaključijo s svojo odgovornostjo, saj je podatek na dokumentu še vedno aktiven in se mora hraniti glede na zakonske ali kako drugače določene minimalne roke hrambe. V tej fazi se morata torej upravljavec in obdelovalec podatkov zavedati, da je potrebno tudi v fazi arhiviranja (hrambe) in uničenja dokumentacije ali ostalih podatkovnih nosilcev zagotoviti varnost in sledljivost v fazi dostopnosti do arhivirane dokumentacije, v fazi same hrambe dokumentacije in na koncu tudi v fazi uničenja dokumentacije ali kakršnegakoli drugega podatkovnega nosilca.

V podjetju Reisswolf smo razvili celovito rešitev, ki upravljavcem in obdelovalcem podatkov omogoča varno in sledljivo upravljanje in obdelavo v celotnem življenjskem ciklu podatka, torej od njegovega nastanka oziroma prejema do njegovega uničenja. Z našo rešitvijo in našimi znanji vam lahko v samo 5 korakih vzpostavimo varen in sledljiv proces upravljanja in obdelave podatkov in

s tem zagotovimo skladnost upravljanja in obdelave podatkov z veljavno zakonodajo, standardi in dobrimi praksami s tega področja, ne glede na vrsto podatka s katerim se upravlja in katerega se obdeluje.

1. Korak: Posnetek stanja in izdelava klasifikacijskega načrta

Nujni pogoj za vzpostavitev dolgoročne celovitosti, sledljivosti in varnosti upravljanja in obdelave podatkov je izdelava posnetka stanja in t.i. Blueprinta s katerim se ugotovi dejansko stanje na področju upravljanja in obdelave podatkov, vrzeli v obstoječem sistemu ter oceni tveganja na tem področju. Posnetek stanja služi kot podlaga za pripravo predlogov izboljšav obstoječega sistema ter definira morebitne nove uporabniške zahteve. Končni rezultat posnetka stanja je izhodni dokument, imenovan klasifikacijski načrt, ki točno definira proces upravljanja in obdelave podatkov, vrste podatkov, razvršča podatke po stopnjah zaupnosti (osebni podatki, posebni osebni podatki, poslovne skrivnosti, tajni podatki ipd.), baze podatkov, način označevanja podatkov, dokumen-

tacije in baz podatkov, nosilce in njihove odgovornosti, načine dostopov do posameznih baz podatkov in same dokumentacije, roke hrambe in ostale posebnosti povezane z upravljanjem in obdelavo podatkov.

2. Korak: Določitev procesa obdelave podatkov

V tej fazi se določi organizacija upravljanja in obdelave podatkov (t.i. Workflow), torej kje posamezni podatki vstopajo v procese, kdo je skrbnik podatkov/baz podatkov, kako poteka proces obdelave podatkov/baz podatkov, kje so vmesne kontrolne točke in kje podatki izstopajo iz procesa. V tem koraku se definirajo tudi načini hrambe podatkov po izhodu iz procesov, torej po zaključku njihove aktivne obdelave. Drugače povedano, določi se proces arhiviranja podatkov in postopke v primeru potrebe po dostopu do arhiviranih podatkov v njihovem času hrambe. Prav tako se v tem koraku določi tudi način trajnega uničenja podatkov, ki se hranijo v fizični obliki (beri dokumentacije) in trajnega izbrisa podatkov, ki se hranijo v e.obliki.



3. Korak: Varna in sledljiva obdelava podatkov

Vzpostavitev organizacije upravljanja in obdelave podatkov je nujni pogoj za zagotavljanje hitre dostopnosti in optimalne uporabne vrednosti podatka. Tako z zakonskega kot tudi poslovnega vidika, pa je v fazi obdelave podatka pomembno zagotoviti njegovo varnost in sledljivost. Pri tem je pomembno, da do podatka dostopajo le tisti, ki so za to pooblaščen in podatek potrebujejo pri izvajanju svojega procesa, da z obdelavo podatka obdelovalci prenehajo takoj, ko prenehajo razlogi za njegovo obdelavo ter, da je ves proces obdelave tudi v vsakem trenutku sledljiv in kot tak omogoča rekonstrukcijo obdelave v primeru pojava zlorabe ali izgube določenega podatka.

4. Korak: Vzpostavitev varnega in sledljivega arhiviranja

V tem koraku določimo pravila arhiviranja podatkov. Tu gre za dve različni področji arhiviranja, odvisno od oblike

podatkovnega nosilca. V kolikor gre za dokumentacijo v fizični obliki je potrebno zagotoviti arhivske prostore, ki so skladni z zahtevami zakonodaje in standardov in kot taki zagotavljajo predvsem varno hrambo dokumentacije in sledljivost upravljanja z dokumentacijo (sledljivost poizvedb za arhivirano dokumentacijo, vnosov in iznosov dokumentacije in rokov hrambe dokumentacije). Gre predvsem za zagotavljanje ustreznih prostorov in opreme, ustreznih klimatskih pogojev (predvsem ustreznega in konstantnega nivoja vlage ter temperature), zavarovanje pred vlomom, požarom, izlivom ali vdorom vode, biološkimi, kemičnimi, fizikalnimi in drugimi škodljivimi vplivi. V kolikor gre za dokumentacijo v e.obliki pa je potrebno poleg varne hrambe in sledljivosti dostopov do dokumentacije upoštevati še varnostna tveganja povezana z dostopnostjo do baz podatkov, kar v zadnjem času, glede na prakse vdorov v informacijske sisteme, predstavlja še posebej velik izziv. Ko govorimo o e.hrambi dokumentacije se mora ves čas hrambe omogočati reprodukcijo vsebine izvirne dokumentacije, dostopnost (varovanje pred izgubo in stalno zagotavljanje dostopa zgolj pooblaščenim uporabnikom), uporabnost (zmožnost reprodukcije in primernost

reprodukcije), avtentičnost (dokazljivost povezanosti reproducirane vsebine z vsebino izvirne dokumentacije) in celovitost (nespremenljivost in neokrnjenost ter urejenost reprodukcije).

5. Korak: Vzpostavitev varnega in sledljivega uničenja

Po zaključenem življenjskem ciklu podatka (izteku roka hrambe) je potrebno poskrbeti za varno in sledljivo uničenje dokumentacije in drugih podatkovnih nosilcev. Ko omenjam druge podatkovne nosilce mislim predvsem razne zdravstvene RTG slike, diske, CD-je, ključke in ostale elektronske prenosne medije, na katerih hranimo dokumente v e-obliki, pa tudi službena oblačila z logotipi podjetij in navedenimi osebnimi podatki. Pomembno se je zavedati, da je življenjski cikel podatka zaključen šele v fazi, ko je ta trajno uničen ali izbrisan in njegova reprodukcija oziroma ponovna rekonstrukcija ni več možna. V tej fazi se zaključi tudi odgovornost upravljavca in obdelovalca po zagotavljanju varne in sledljive obdelave podatkov.

Težko je v nekaj odstavkih opisati kompleksen pristop k vzpostavljanju varnega in sledljivega upravljanja in obdelave podatkov, saj gre za izjemno kompleksno področje, tako z vidika zakonodaje in standardov, kot tudi specifičnosti uporabniških potreb posamezne organizacije. Vsekakor je pomembno, da se v prvi vrsti zagotovi skladnost upravljanja in obdelave z zakonodajo in standardi, nato pa se z izborom ustrezne organizacije ter tehničnih in varnostnih ukrepov vzpostavi celovit sistem, ki nam v vsakem trenutku zagotavlja sledljivo obdelavo in varno hrambo ne glede na to v katerem življenjskem ciklu se določen podatek obdeluje.

V Reisswolfo smo zato razvili enostaven, ekonomsko in uporabniško učinkovit, varen in sledljiv sistem upravljanja z dokumentacijo tako v fizični kot tudi e.obliki, ki uporabnikom zagotavlja skladnost upravljanja in obdelave dokumentacije z zakonodajo, standardi in dobrimi praksami. ■

