IIA – Inštitut notranjih revizorjev

Svetovalni napotek 2130-A1-2:
Ocenjevanje okvira zasebnosti v organizaciji

Temeljni standard v tej zvezi

2130.A1 – Notranja revizija mora ovrednotiti ustreznost in uspešnost kontrol pri odzivanju na tveganja za upravljanje, delovanje in informacijske sisteme organizacije, pri čemer upošteva:

- doseganje strateških ciljev organizacije,
- zanesljivost in neoporečnost računovodskih in izvajalnih informacij,
- uspešnost in učinkovitost delovanja in programov,
- varovanje premoženja,
- skladnost z zakoni, drugimi predpisi, usmeritvami, postopki in pogodbami.

---

1. Nezavarovanje osebnih informacij s primernimi kontrolami ima lahko pomembne posledice za organizacijo. Škoduje lahko ugledu posameznikov in/ali organizacije ter izpostavlja organizacijo tveganjem, ki vključujejo pravno odgovornost in zmanjšanje zaupanja potrošnikov in/ali zaposlencev.

2. Opredelitev zasebnosti se razlikuje glede na kulturo, politično okolje in zakonodajni okvir držav, v katerih deluje organizacija. Tveganja, ki so povezana z zasebnostjo informacij, vključujejo zasebnost osebe (fizično in psihološko), zasebnost prostora (svobodo pred nadzorovanjem), zasebnost sporočanja (svobodo pred opazovanjem) in zasebnost informacij (zbiranje, uporabo in razkritje osebnih informacij s strani drugih). Osebne informacije se na splošno nanašajo na informacije, povezane z določeno osebo, ali na prepoznane značilnosti, ki so v povezavi z drugimi informacijami lahko povezane z določeno osebo. Vključujejo lahko katerekoli dejanske ali subjektivne informacije – evidentirane ali ne – v katerikoli medijski obliki. Osebne informacije so med drugim lahko:

   - ime, naslov, identifikacijske številke, družinska razmerja,
   - osebne mape zaposlenih, njihove ocene, vpisani zaznamki, socialni položaj ali disciplinski ukrepi,
   - evidence o kreditih, dohodek, finančni položaj,
   - zdravstveno stanje.

3. Uspešno kontroliranje varstva osebnih informacij je bistvena sestavina upravljanja organizacije, upravljanja tveganj in kontrolnih postopkov organizacije. Organ nadzora je končno odgovoren za prepoznavanje glavnih tveganj za organizacijo in za uvedbo primernih kontrolnih postopkov za zmanjšanje takih tveganj. To vključuje vzpostavitev potrebnega okvira zasebnosti za organizacijo in spremljanje njegovega uresničevanja.

4. Notranja revizija lahko prispeva k dobremu upravljanju organizacije in upravljanju tveganj s presojanjem primernosti poslovodskega prepoznavanja tveganj, ki se nanašajo na cilje zasebnosti v organizaciji in primernost kontrol, ki so vzpostavljene za zmanjšanje takih tveganj na sprejemljivo raven. Notranja revizija ima dober položaj za ocenjevanje okvira zasebnosti v svoji organizaciji in za prepoznavanje pomembnih tveganj ter tudi za dajanje primernih priporočil za njihovo zmanjšanje.

5. Notranji revizor ugotovi vrsto in primernost informacij, ki so zbrane v organizaciji in za katere meni, da so osebne ali zasebne, kakšne so uporabljene metode zbiranja in ali je uporaba takih informacij v organizaciji v skladu z nameravano uporabo in veljavno zakonodajo.

6. Glede na zelo strokovno in pravno naravo vprašanj zasebnosti potrebuje notranji revizor primerno znanje in sposobnosti za presojo tveganj in kontrol okvira zasebnosti v organizaciji.

7. Pri ocenjevanju upravljanja okvira zasebnosti v organizaciji notranji revizor:

   - upošteva zakone, druge predpise in usmeritve, ki se nanašajo na zasebnost v pravnem redu države, v kateri deluje organizacija;
   - sodeluje s pravnim svetovalcem v organizaciji pri natančnem ugotavljanju vrste zakonov, drugih predpisov in drugih standardov ter ravnanja, ki veljajo za organizacijo in državo/države, v kateri/-h organizacija deluje;
   - sodeluje s strokovnjaki za informacijsko tehnologijo pri ugotavljanju, ali so varovanje informacij in kontrole za varstvo podatkov vzpostavljeni in se redno pregledujejo ter presojajo glede primernosti;

- upošteva raven ali zrelost ravnanja glede zasebnosti v organizaciji. Glede na to raven so vloge notranjega revizorja pri tem lahko različne. Revizor lahko prispeva k lažjemu razvijanju in uporabi programa zasebnosti, ocenjuje poslovodsko presojanje tveganja zasebnosti za določitev potreb in izpostavljenosti tveganju v organizaciji ali daje zagotovila o uspešnosti usmeritev glede zasebnosti, ravnanja in kontrol v vsej organizaciji. Če notranji revizor prevzame kakršno koli odgovornost za pripravo in uvajanje programa zasebnosti, bo neodvisnost notranjega revizorja oslabljena.

Objavljeno januarja 2009.

***