Begrundelser for afvigelserne i Visma FirstAgenda's ISAE3000 erklæring 2023/2024

AD B.6 - Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor:
For 4 ud af 8 produkter har det ikke været muligt at få en liste over brugere fra systemet. De 4 produkter vedrører:

► FirstAgenda Live

► FirstAgenda Management

► FirstAgenda Publication

► Letdialog.

Vores begrundelse:

Afvigelsen skyldes en ændring i proceduren hos den uafhængige revisor. Vi gør opmærksom på at der fortsat er formaliseret forretningsgange for tildeling og afbrydelse af brugeradgange til personoplysninger, samt at vi ikke har foretaget ændringer til hverken proceduren eller implementeringen heraf siden sidste erklæring, hvor den var uden anmærkning. Der var desværre ikke en enighed om hvordan dette bedst blev dokumenteret hvorfor vi til sidst accepterede kommentaren fra den uafhængige revisor

AD B.10 - Personoplysninger, der anvendes til udvikling, test eller lignende, sker altid efter af tale med dataansvarlig. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne:
Det har ikke været muligt at modtage dokumentation for, at data er anonymiseret eller at produktionsdata ikke anvendes til test uden aftale med kunden.

Vores begrundelse:

Afvigelsen skyldes en ændring i proceduren hos den uafhængige revisor. Vi gør opmærksom på at der fortsat ikke anvendes personoplysninger, herunder produktionsdata til test samt at vi ikke har foretaget ændringer til hverken proceduren eller implementeringen heraf siden sidste erklæring, hvor den var uden anmærkning. Der var desværre ikke en enighed om hvordan dette bedst blev dokumenteret hvorfor vi til sidst accepterede kommentaren fra den uafhængige revisor.

AD B.11 - De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og/ eller penetrationstests:
Der er ikke udført penetrationstest i erklæringsperioden.

Vores begrundelse:

Vi er en del af Vismas sikkerhedsprogram (Visma Security Program) som løbende foretager sårbarhedsscanninger og penetrationstests. Det er som en del af programmet ikke muligt at videregive disse test idet de ikke viste sårbarheder. Vi kan bekræfte, at alle tests er blevet udført korrekt. Denne afvigelse er derfor et resultat af uenighed mellem os som leverandør og den uafhængige revisor om hvad der udgør et passende revisorspor.

AD B.12 - Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches:
For 4 ud af 25 stikprøver på ændringer, er der ikke dokumentation på test og godkendelse.
For 5 ud af 5 stikprøver på udvalgte 5 uger på patches, er der ikke dokumentation, der viser, at patches er fuldført i de givne uger.

Vores begrundelse:

De 4 stikprøver uden dokumentation på test og godkendelse skyldes at det var opgaver, som var startet op, men undervejs er blevet nedlagt, da rettelsen alligevel ikke var relevant. Opgaven er derfor blevet afsluttet og nedlagt uden test og godkendelse.

For de 5 ud af 5 stikprøver skyldes afvigelsen en ændring i proceduren hos den uafhængige revisor. Vi gør opmærksom på at der fortsat er fastlagte procedurer som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches samt at vi ikke har foretaget ændringer til hverken proceduren eller implementeringen heraf siden sidste erklæring, hvor den var uden anmærkning. Der var desværre ikke en enighed om hvordan dette bedst blev dokumenteret hvorfor vi til sidst accepterede kommentaren fra den uafhængige revisor.

AD B.13 - Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov:
Det har ikke været muligt at få en fuldstændig liste til understøttelse af den udførte periodiske gennemgang af brugere med adgang til systemerne.

Vores begrundelse:

Afvigelsen skyldes en ændring i proceduren hos den uafhængige revisor. Vi gør opmærksom på at der fortsat er formaliseret forretningsgange for tildeling og afbrydelse af brugeradgange til personoplysninger, samt at vi ikke har foretaget ændringer til hverken proceduren eller implementeringen heraf siden sidste erklæring, hvor den var uden anmærkning. Der var desværre ikke en enighed om hvordan dette bedst blev dokumenteret hvorfor vi til sidst accepterede kommentaren fra den uafhængige revisor.