IT-SIKKERHED PÅ RIVAL A/S (RIVAL)

BEHANDLING AF PERSONDATA I TILKNYTNING TIL MEDARBEJDERE PÅ RIVAL

RIVAL indsamler kun de nødvendige personoplysninger til specifikke og saglige formål. Der henvises til RIVALs Privatlivspolitik, hvori er beskrevet hvilke personoplysninger der behandles mv.

RIVAL er dataansvarlig for de personoplysninger, der behandles.

Der behandles persondata i Microsoft Active Directory (navn og stilling) og i Exchange (navn, intern mailadresse). Derudover behandles persondata i Navison. Endelig behandles data på netværket i brugernes egne og fælles mapper, styret af Microsoft NTFS-rettigheder.

ADGANGSBEGRÆNSNING OG KONTROL

Rettighedsstyring for login til IT-systemet håndteres via Login i Microsoft Active Directory. Der er separat brugeroprettelse og passwords i Navision, da der kræves særskilt login hertil.

Forsøg på uautoriseret login kan ses i serverens event-viewer. Der bliver pt. Ikke logget ændringer af fil-data, da brugerne har begrænsede rettigheder.

INTEGRITET, FORTROLIGHED OG TILGÆNGELIGHED

Med henblik på at sikre, at personoplysningerne er pålidelige og ikke bevidst eller ved tilfældighed kan ændres under en behandling, ved opbevaringen eller evt. overførsel (fx backup), er det kun udvalgte personer, der har rettighed til at ændre i brugerdata. Backuppen er krypteret og går 1 år tilbage.

Backuppen er krypteret med 256 bit kryptering for at sikre personoplysningernes fortrolighed.

Ved udveksling af personoplysninger og for at sikre datas integritet og fortrolighed er der mulighed for modtagelse og afsendelse af sikker mail, hvis det er nødvendigt. Ved ekstern adgang (fjernskrivebord) benyttes SSL-kryptering.

DE REGISTREREDES RETTIGHEDER

Der kan søges på en navngivet person og lokaliseres data om personen via Microsoft Active Directory på Domain kontrolleren og i Navision.

Personoplysninger og brugere kan slettes i Microsoft Active Directory og fil data kan eksporteres/slettes. Mails kan eksporteres ud af Exchange i en pst-fil.

Alle personoplysninger er som udgangspunkt fortrolige.

Personoplysninger om fratrådte medarbejdere slettes efter det indeværende kalenderår + 5 år efter fratrædelse, med mindre det er nødvendigt, at oplysningerne opbevares i længere tid. Dette kan eksempelvis være tilfældet ved arbejdsskader eller ved forsvarelse af retskrav.

Såfremt en registreret person anmoder om "Retten til at blive glemt", slettes oplysninger om den pågældende i Navision og i Microsoft Active Directory. En bruger og brugerens mailboks kan slettes i AD og Exchange.

REGLER OM SLETNING

Der er ikke en funktion i IT systemet, hvor man kan angive sletteperiode samt kriterier for sletning (deletion triggers) for bestemte oplysninger og hvor systemet herefter automatisk foretaget sletning af oplysningerne.

Der er etableret manuelle procedurer, der sikrer, at oplysningerne slettes. Der følges op på dette, når backup-data er ældre end 1 år. Dette er en del af den manuelle arbejdsprocedure.

Der er ikke en funktion, der sletter personoplysninger efter en angivet periode.

Tekniske foranstaltninger er implementeret for at sikre, at oplysningerne slettes forsvarligt, bl.a. ved backupdata, hvor de nye data overskriver de gamle data.

FORSVARLIG PLACERING AF PERSONDATA

Såvel hovedserver som backup-server er placeret i et særskilt, nedkølet serverrum. Der er ikke adgang hertil, uden at man går igennem ejendommens yderdør og selvstændig aflåst dør til serverrum, hvortil kun særligt betroede medarbejdere har nøgle (to låste døre).

Serveren bliver løbende opdateret hver 14. dag efter behov. Alle servere bliver opdateret helt mindst en gang om måneden.

Hele virksomhedens IT er bygget op omkring Microsoft Active Directory, hvorigennem alle bruger- og adgangsrettigheder styres. Navision-adgangen bliver styret separat. Forbindelsen til Internettet beskyttes af en Microsoft TMG firewall. Hver 14. dag bliver servernes logger og netværket

gennemgået for mistænkelig aktivitet. Alle klienter har installeret Symantec Endpoint Protection og opdateres og overvåges fra en central antivirus server.

Alt data er placeret på hovedserveren, som befinder sig i et særskilt aflåst lokale. Uden for arbejdstid er de ydre lokaler herom beskyttet af aflåst hoveddør.

Der bliver foretaget backup af alt data hver arbejdsdag kl 22:00, som efterfølgende bliver transporteret ud af huset via USB 1 gange om ugen. Alt data er krypteret med 256 bit og befinder sig kun i Danmark.