Indhold

Rettighedsstyring - hvem skal have adgang?

Autorisering og brugeradministrering i din organisation

Hvorfor er rettighedsstyring vigtigt?

Effektive procedurer for autorisering og brugeradministrering er afgørende for it- og informationssikkerheden i din organisation. Ligesom du holder styr på, hvem der har nøgle til dit hjem, og hvem der skal have nøglen til dit arkivskab, skal du holde styr på, hvem der har adgang til dine systemer og til hvilke oplysninger – og at de ved hvordan oplysningerne skal behandles. Det er vigtigt for persondatasikkerheden, for medarbejdere, kunder og for borgere, men det er også med til at beskytte din forretning.

Databeskyttelsesforordningen (GDPR) indeholder regler om behandlingssikkerhed samt databeskyttelse gennem design og standardindstillinger. Disse regler benytter en risikobaseret tilgang til sikkerhed, hvor et passende sikkerhedsniveau etableres ved hjælp af "passende tekniske og organisatoriske foranstaltninger".

Styring af brugeres adgange til data er en så basal del af informationssikkerhed – og dermed også behandlingssikkerhed inden for databeskyttelse – at det kan læses direkte ud af principperne i databeskyttelsesforordningens artikel 5, stk. 1, litra f.

Databeskyttelsesforordningens artikel 5, stk. 1, litra f.

Personoplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«).

Datatilsynet får løbende kendskab til mange brud på persondatasikkerheden, som skyldes mangelfuld rettighedsstyring. Denne vejledning giver eksempler på situationer, hvor mangelfuld rettighedsstyring fører til sikkerhedsbrud og anviser dig muligheder for at imødegå dem.

Hvem skal have styr på rettighedsstyring?

Det korte svar er, at det skal alle, der anvender it-systemer, som indeholder personoplysninger! Databehandlere som drifter it-systemer skal også have styr på kravene og kan selvstændigt pådrage sig ansvar.

- **Ledelsen**. Det er ledelsens ansvar at sikre, at der arbejdes aktivt med rettighedsstyring, især autorisering og brugeradministrering i organisationen gennem etablering af fornødne procedurer og tildeling af tilstrækkelige ressourcer til en effektiv opgaveløsning. Hvor meget der skal til, bestemmes primært af risikovurderingen for behandlingen af personoplysninger i din organisation.

- **DPO (Data Protection Officer, Databeskyttelsesofficer).** Som DPO skal du overvåge beskyttelsen af personoplysninger i din organisation, fx om der er etableret passende procedurer og tekniske foranstaltninger mod uautoriseret eller ulovlig adgang til personoplysninger[1].

- **Medarbejdere med ansvar for it-sikkerhed.** Det er en helt grundlæggende del af opgaven med it-sikkerhed, at sikre, at der effektivt tages stilling til og løbende føres kontrol med, at adgangsrettigheder til it-systemer og personoplysninger passer til det arbejdsmæssige behov, og at rettighederne ikke skaber unødige muligheder for misbrug.

- **Medarbejder uden ansvar for it-sikkerhed.** Som medarbejder kan du støtte op om din organisations forpligtelser ved at være opmærksom på, om dine rettigheder revideres, når du skifter afdeling eller får nye opgaver.

Kommentar [F1]: Det giver anledning til tvivl, hvorvidt denne sætning henviser til arbejdet med rettighedsstyring eller tildeling af tilstrækkelige resurser til opgaveløsning.

Katalog med relevante foranstaltninger

Vejledningen er koblet til et katalog, der beskriver tekniske og organisatoriske foranstaltninger, som er relevante at overveje for at sikre en god og ansvarlig rettighedsstyring i overensstemmelse med kravene i databeskyttelsesforordningens artikel 32.

[1] Databeskyttelsesforordningens artikel 39, stk. 1, litra b, samt artikel 5, stk. 1, litra f.

Databeskyttelsesforordningen. Personoplysningssikkerhed.

Artikel 32 (Behandlingssikkerhed)

Stk. 1. Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:

a) pseudonymisering og kryptering af personoplysninger

b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

Kataloget fungerer som et opslagsværk. For hver foranstaltning er der angivet risici, som foranstaltningen er rettet imod, samt implementeringsforslag. Endvidere er der en vejledning til vurdering af foranstaltningens relevans. Foranstaltningerne i kataloget er i høj grad baseret på erfaringer fra tilsyn i private og offentlige virksomheder, brud på persondatasikkerheden anmeldt til Datatilsynet, EDBP's retningslinjer om artikel 25[2], samt ISO-standarderne 27001[3] og 27002. ISO-standarderne er internationale standarder for informationssikkerhed, som følges af de fleste offentlige myndigheder og mange private virksomheder, og er udtryk for et internationalt anerkendt niveau for sikkerheden ved anvendelse af informationsteknologi.

Kommentar [F2]: Vi vil foreslå, at vejledningen skal kunne læses uafhængigt af kataloget.

Centrale begreber

Autorisation: Fuldmagt, godkendelse – udstedt af en autoritet, fx en leder.

At autorisere: At bemyndige, godkende.

Uautoriseret adgang: En adgang som ikke er autoriseret (godkendt). Det kan fx opstå hvis:

- En autorisation udløber, uden at adgangen lukkes.
- Ved en fejl gives adgang til alle ansatte i stedet for kun de ansatte, som var autoriserede.
- Ved en fejl lægges data på internettet – hvorved reelt hele verden får uautoriseret adgang.
- En hacker misbruger svagheder i et it-system og opnår derved adgang til data.

Bemærk, at det er uafhængigt af, om adgangen er anvendt eller ej. Man kan altså have haft uautoriseret adgang til data uden nogensinde at have tilgået de data, som der var adgang til.

Kommentar [F3]: Forskellen på rettighedsstyring, brugerstyring og autorisation bør forklares her.

Det bør forklares, at brugerstyring styrer hvem og hvornår, og rettighedsstyring hvilke adgange der er givet til de enkelte systemer.

Kommentar [F4]: Layout af boksen virker ikke sammenhængende og bør justeres, så den understøtter læseren i forståelsen af vejledningen.

[2] 4/2019 om artikel 25 - Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger - Version 2.0

[3] Dansk Standard DS/ISO/IEC 27001 – Krav til Informationsteknologi – sikkerhedsteknikker – Ledelsessystemer for informationssikkerhed (ISMS)

Autorisationsansvarlig: En person, som er udpeget til at kunne autorisere og dermed godkende andres adgange til fx it-systemer og software.

Brugeradministrator: En person, som er udpeget til at tildele andre personer adgang og rettigheder i ét eller flere it-systemer eller fysiske adgangsmedier, hvor denne tildeling sker på baggrund af en autorisation.

Brugeradministrering: Brugeradministrering er en proces, der normalt består af i høj grad organisatoriske foranstaltninger, som skal sikre, at kun de rigtige personer har en nøgle til døren, en adgangskode til it-systemet, osv. Men der kan også være tekniske foranstaltninger, der hjælper brugeradministratoren igennem processen, forhindrer fejl, samt dokumenterer, at opgaver er udført i henhold til anmodninger/godkendelser fra en autorisationsansvarlig.

Adgangsstyring og adgangsrettigheder: Begrebet "adgangsstyring" omfatter en sikring af, at:

1) Adgang til fx personoplysninger er autoriseret (godkendt af en autoritet) og,
2) Adgangen er begrænset til, hvad der er behov for til arbejdsmæssige formål, og som samtidig er forsvarligt rent sikkerhedsmæssigt.

Denne vejledning handler primært om, hvordan man sikrer punkt 2, og denne underdel kaldes styring af adgangsrettigheder, fordi det ikke kun handler om, hvad brugerne får "adgang" til af data, men også hvad brugerne *kan* med disse data – læse, ændres, slette, osv. Man kan også sige, at punkt 1 handler om, at give brugeren mulighed for log-in, hvad enten det er med et password, en fysisk nøgle til en dør, eller andet, mens punkt 2 handler om, hvad brugeren kan "bag" dette log-in.

Foranstaltning: Handling eller initiativ som iværksættes for at fremme en ønsket udvikling eller modvirke en uønsket udvikling. Det svarer til det, som it-sikkerhedsstandarden ISO 27001 betegner som "kontroller" og kan også beskrives som aktiviteter der styres og vurderes løbende. En foranstaltning kan være *forebyggende*, *opdagende* eller *korrigerende* eller en kombination af disse.

Tekniske foranstaltninger med relevans for rettighedsstyring er fx it-løsninger til brugeradministrering, automatisk kryptering/sletning, automatisk adgangskontrol (log-in), registrering af anvendelser af personoplysninger (logning), ~~fysiske døre og låse~~.

Organisatoriske foranstaltninger med relevans for rettighedsstyring er fx sikkerhedspolitikker, procedure for jævnlig kontrol af adgangsrettigheder, procedure for inddragelse af adgangsrettigheder ved fratrædelse, opgavefordeling efter kompetencer, uddannelse i korrekt anvendelse af it-løsninger, vurdering og evaluering af effektiviteten af tekniske og organisatoriske foranstaltninger.

Registrerede: De fysiske personer, hvis personoplysninger er genstand for en behandling.

Kom godt i gang – skab overblik og vurdér risici ved din behandling af personoplysninger

Inden for it-sikkerhed handler rettighedsstyring typisk om interne procedurer og tekniske foranstaltninger, der styrer *tildeling, ændring* og *fratagelse af* rettigheder i de it-systemer, man anvender i sin organisation. Databeskyttelsesforordningen vedrører dog også fysiske dokumenter/registre, som indeholder personoplysninger.

Før du kan gå i gang, skal der være et *overblik* over det samlede it-miljø. Dette er en forudsætning for at kunne vurdere, hvilke foranstaltninger det giver mening at implementere, og om det er din egen organisation eller en ekstern leverandør, der skal udføre det. Det er fx relevant at vide, hvad der skal til for at kunne lukke adgange hurtigt, når det er aktuelt, dvs. om der findes decentral rettighedsstyring udført af egne medarbejdere eller om adgange skal lukkes via en ekstern databehandler. Risici ved decentral rettighedsstyring kan ses af nogle af risikoscenarierne, som er beskrevet senere, og ved at læse om den afhjælpende foranstaltning "Centraliseret rettighedsstyring" i kataloget over foranstaltninger.

Kommentar [F5]: Vi mener ikke at denne sondring er nødvendig, da begge delelementer adresseres ifm. tilkendelse af brugerrettigheder.
Hvis sondringen er væsentlig for forståelsen af vejledningen, vil vi foreslå, at tilgangen præsenteres i vejledningens indledning.

Kommentar [F6]: Er ikke tekniske foranstaltninger.

Kommentar [F7]: KL er ikke enig i, at det kræver overblik over det samlede it-miljø, før man kan gå i gang med arbejdet med rettighedsstyring. Det er vigtigt at få styr på sin brugerstyring, inden det samlede overblik er på plads.

Både overblikket over it-miljøet og eksisterende foranstaltninger kan evt. allerede være afdækket gennem organisationens efterlevelse af reglen i databeskyttelsesforordningens artikel 30 angående "fortegnelse over behandlingsaktiviteter". it-sikkerhedsstandarden ISO 27001 stiller ligeledes krav om "fortegnelse", men for "aktiver", hvilket bl.a. omfatter data, herunder personoplysninger. Det vil typisk være it-afdelingen, som fører fortegnelser over aktiver som led i deres efterlevelse af relevante it-sikkerhedsstandarder.

Visse tekniske og organisatoriske foranstaltninger kan blive implementeret via de værktøjer, der kan anvendes til brugeradministrering. Identity Access Management (IAM) og Privileged Access Management (PAM) er typer af systemer, som kan automatisere foranstaltninger angående rettighedsstyring.

Denne vejledning er en hjælp til at håndtere de mest gængse sikkerhedstrusler og problemstillinger i relation til rettighedsstyring i din organisation. Alle sikkerhedskrav efter databeskyttelsesforordningen forudsætter, at det er vurderet, hvilke trusler en behandling er udsat for, og hvilke risici dette udgør for personoplysningssikkerheden.

Databeskyttelsesforordningens artikel 32, stk. 2

Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Vejledningen giver dig relevante input til din organisations risikovurdering med beskrivelser af relevante risiko-scenarier og anbefalinger af mulige tekniske og organisatoriske foranstaltninger, som vil kunne mindske disse risici.

Vurdering af hvilket sikkerhedsniveau som kan anses for passende i netop din organisation, kræver dog en konkret risikovurdering efter databeskyttelsesforordningen, som ikke er temaet for denne vejledning.

Hvornår går det galt? Eksempler fra danske virksomheder og myndigheder

Ransomware – når data holdes som gidsel

Her påvirkes de registreredes rettigheder direkte gennem manglende tilgængelighed til personoplysninger og ofte også manglende fortrolighed.

I de seneste år er flere og flere organisationer blevet ramt af ransomware. Der er tale om ondsindede angreb, hvor hackere udnytter sårbarheder i it-systemer eller snyder medarbejdere gennem phishing eller anden form for 'social engineering' for at opnå adgang til data på it-systemerne, kryptere data, og forlange løsepenge for at dekryptere dem. Ofte sker det først efter, at data er udtrukket af it-systemerne og, hvis løsesummen ikke betales, kan der i stedet afpresses under trussel om at offentliggøre data. Der ses også flere og flere eksempler på, at data sælges videre af hackerne og derefter anvendes til svindel og identitetsmisbrug til skade for de registrerede personer, eller de registrerede bliver selv udsat for afpresning.

Mange foranstaltninger er relevante for at opbygge et tilstrækkeligt forsvar mod ransomware-angreb – især backup af it-systemer/data og forsvar mod cyberangreb. Betaling af løsesummen hjælper sjældent. Men uanset om man har en god backup – og dermed er i stand til at reetablere sine it-systemer og data – så

Kommentar [F8]: Se kommentaren ovenfor om it-miljø.

Kommentar [F9]: Kommunerne skal kun følge principperne i ISO.

Kommentar [F10]: Det er overvejet at sætte dette afsnit til sidst. Hvad synes du? Overvej evt. strukturen generelt.

Kommentar [F11]: Disse kursiverede forklaringer med udgangspunkt i databeskyttelsesforordningens begreber er svært tilgængeligt sprog.

beskytter det ikke imod misbrug af de udtrukne data. Meget af udgiften ved et en succesfuldt ransomware-angreb ligger desuden i reetableringen af it-systemerne via backup.

Begrænsning af adgangsrettigheder – især privilegerede rettigheder – kan evt. forhindre et succesfuldt ransomware-angreb, da hackere ofte har brug for at opnå særlige rettigheder i it-systemerne for at kunne udføre angrebet. Hvis angrebet alligevel er succesfuldt, kan begrænsede adgangsrettigheder mindske skaden ved angrebet, fordi angrebet derved kan nå færre it-systemer. Det er dog vigtigt at bemærke, at foranstaltningerne beskrevet i denne vejledning ikke kan stå alene, når det angår beskyttelse mod ransomware.

Kommentar [F12]: Afsnittet bør udgå af vejledningen for at skærpe fokus på rettighedsstyring.

Kommentar [F13]: Forklar gerne dette begreb.

Kommentar [F14]: Dette afsnit kan med fordel indarbejdes i det indledende afsnit om "Hvorfor er rettighedsstyring vigtigt?"

Relevante foranstaltninger

- *Adgangsrettigheder efter behov*
- *Awareness*
- *Automatisk lukning af inaktive adgange*
- *Centraliseret rettighedsstyring*
- *Dataadgang efter behov*
- *Forlods angivelse af adgangslukning*
- *Funktionsadskillelse*
- *Kontrolleret/forhindret dublering af adgangsrettigheder*
- *Kontrolleret/forhindret genanvendelse af autorisation*
- *Minimering af privilegerede adgangsrettigheder*
- *Periodisk kontrol af adgangsrettigheders aktualitet*
- *Pseudonymisering, anonymisering*
- *Tilpasning af adgangsrettigheder ved ændring af ansættelse*

[Indsæt link til offentliggjorte afgørelser vedrørende sikkerhedsbrud pga. ransomware]

Manglende adgangsbegrænsning

Her påvirkes de registreredes rettigheder direkte gennem manglende fortrolighed.

Kommentar [F15]: Disse kursiverede forklaringer med udgangspunkt i databeskyttelsesforordningens begreber er svært tilgængeligt sprog.

En medarbejder opsætter en mappe på et serverdrev og placerer nogle fortrolige kundedata eller HR-oplysninger, som kun skal kunne ses af særligt udvalgte HR-medarbejdere. Manglende viden om eller opmærksomhed på korrekt opsætning af adgangsrettigheder indebærer, at uautoriserede personer kan tilgå de fortrolige oplysninger.

Et andet eksempel er udskiftning af eller ændringer på en server uden sikring af, at den aktuelle adgangsbegrænsning aktivt videreføres ved ændringen, hvilket skaber uautoriseret adgang. Den manglende videreføring kan f.eks. skyldes manglende viden om den pågældende adgangsbegrænsning eller manglende test.

Mangler i adgangsbegrænsning kan ske på grund af fejl og manglende test, eller fordi ændringsbegrænsningen er lavet autonomt af en medarbejder eller enhed uden styring fra centralt hold. Konsekvensen er typisk, at mange eller alle medarbejdere via det interne net – eller hele verden via internettet – fik uautoriseret adgang til beskyttelsesværdige personoplysninger.

Der går ofte meget lang tid, nogle gange flere år, inden denne type brud på persondatasikkerheden opdages, fordi de autoriserede brugere ikke bemærker, at andre end de relevante har adgang.

Relevante foranstaltninger

- *Adgang koblet til viden*
- *Centraliseret rettighedsstyring*
- *Ændringsstyring (Change Management)*

[Indsæt link til offentliggjorte afgørelser vedrørende sikkerhedsbrud pga. manglende adgangsbegrænsning]

Når misforståelser eller manglende viden fører til fejl

Her påvirkes de registreredes rettigheder direkte gennem manglende fortrolighed.

Pædagoger på en daginstitution fik rettigheder til at arkivere breve med følsomme personoplysninger i kommunens ESDH-system. Nogle brugere misforstår betydningen af et "flueben" og kommer utilsigtet til at sætte brevet til automatisk at blive offentliggjort i en postliste på kommunens hjemmeside. Derved får hele verden øjeblikkeligt uautoriseret adgang til indholdet i brevet. Problemet i denne type sikkerhedsbrud er, at der uddelegeres opgaver uden hensyntagen til, hvilken viden der kræves. Det kan evt. være fordi det umiddelbart virker som en besparelse i administrative omkostninger, men sikkerheden er altså ikke med i regnestykket.

Fordi brugeren ikke selv ved, at noget er gjort galt, kan der ved denne type brud på persondatasikkerheden, gå lang tid inden det opdages.

Relevante foranstaltninger

- *Adgang koblet til viden*
- *Awareness*

[Indsæt link til offentliggjorte afgørelser vedrørende sikkerhedsbrud pga. misforståelse mv.]

Misbrug af superbrugerrettigheder

Her påvirkes de registreredes rettigheder ikke direkte, men indirekte i kraft af afledte konsekvenser.

En offentlig styrelse blev udsat for svindel i millionklassen gennem misbrug af tilskudsmidler. Svindlen var mulig pga. en enkelt medarbejders misbrug af tildelte "superbrugerrettigheder", der bl.a. gjorde det muligt at frakoble alarmer og gå ind i mange forskellige systemer og sætte godkendelsesprocedurer og andre foranstaltninger ud af kraft. Selv om sagen vedrørte en offentlig styrelse, kunne den fx have afledte menneskelige konsekvenser, hvis værdige modtagere går glip af et offentligt tilskud. Sagen er et eksempel på at tildeling af mange rettigheder uden effektive kontrolforanstaltninger kan udgøre en sårbarhed, der let kan udnyttes.

Relevante foranstaltninger

- *Minimering af privilegerede adgangsrettigheder*
- *Funktionsadskillelse*
- *Centraliseret rettighedsstyring*
- *Adgangsrettigheder efter behov*
- *Logning af brugeradministrators handlinger*
- *Stikprøver i log over brugeradministrators handlinger*

[Indsæt evt. link til offentliggjorte afgørelser af relevans for risikoscenariet]

Kommentar [F16]: Vi mener ikke dette er et godt eksempel på brugerstyring. Det er jo snarere forkert brug af systemet, end det er en brugerstyringsproblematik.

Kommentar [F17]: Disse kursiverede forklaringer med udgangspunkt i databeskyttelsesforordningens begreber er svært tilgængeligt sprog.

Kommentar [F18]: Disse kursiverede forklaringer med udgangspunkt i databeskyttelsesforordningens begreber er svært tilgængeligt sprog.

CEO fraud og fakturasvindel

Her påvirkes de registreredes rettigheder ikke direkte, men evt. indirekte i kraft af afledte økonomiske eller aftalemæssige konsekvenser.

CEO-fraud, også kendt som direktørsvindel eller BEC (Business Email Compromise), er falske mails eller SMS'er, der er formuleret som om de er afsendt af en direktør eller leder. De it-kriminelle forsøger gennem falske mails at narre medarbejdere til at betale falske fakturaer eller overføre beløb til en specifik bankkonto.

Selv om eksemplet umiddelbart kun har en økonomisk konsekvens, kan det påvirke virksomhedens økonomi så meget, at det går ud over virksomhedens drift og de ansatte helt generelt. Hvis virksomheden fx er en offentlig myndighed med et ansvar over for borgere eller et privathospital, kan det også ramme personer uden for virksomheden.

Relevante foranstaltninger

- *Adgangsrettigheder efter behov*
- *Adgang koblet til viden*
- *Awareness*

[Indsæt evt. link til offentliggjorte afgørelser af relevans for risikoscenariet]

Undgå svage led – brug en kombination af foranstaltninger

Eksemplerne tager udgangspunkt i konkrete sikkerhedsbrud og angår både utilsigtede fejl og ondsindede handlinger. I begge tilfælde er de beskrevne foranstaltninger i denne vejledning relevante at forholde sig til.

Fælles for mange af de brud på persondatasikkerheden, som Datatilsynet tager stilling til, er, at de kun kan undgås gennem en kombination af flere foranstaltninger, som tilsammen etablerer et passende sikkerhedsniveau, fordi der ellers kan være et svagt led i "sikkerhedskæden".

Gruppering af foranstaltninger efter opgaver i organisationen

I nogle arbejdsmæssige situationer er det særligt relevant at skærpe opmærksomheden på autorisering og brugeradministrering for at etablere eller opretholde de foranstaltninger, der skal sikre god rettighedsstyring.

Nedenfor grupperes en række foranstaltningerne i forhold til *hvilken opgave*, der skal udføres i organisationen.

Nogle gange bliver dele af opgaven med rettighedsstyring udført hos en leverandør (typisk en databehandler). Her kan organisationen ikke direkte styre, hvilke foranstaltninger, der implementeres eller hvordan. I den situation kan de beskrevne foranstaltninger i stedet beskrives i en databehandleraftale, eller den dataansvarlige må på anden vis sikre sig, at god rettighedsstyring opretholdes.

Etablering af brugeradministration

På det tidspunkt, hvor organisationen etablerer en enhed, som får til opgave at styre adgangsrettigheder dannes fundamentet for de principper, hvorefter man vil styre adgangsrettigheder. Derfor skal der på dette

Kommentar [F19]: Bør udgå, da det ikke har med rettighedsstyring at gøre.

Kommentar [F20]: Disse kursiverede forklaringer med udgangspunkt i databeskyttelsesforordningens begreber er svært tilgængeligt sprog.

Kommentar [F21]: Her kan med fordel nævnes tilsyn og kontrolrapporter.

tidspunkt være gjort overvejelser om, hvilke procedurer, værktøjer, rollefordelinger, osv. der skal anvendes for at sikre god rettighedsstyring.

[GRAFIK: hus med personer og dokumenter]

Relevante foranstaltninger

- *Funktionsadskillelse*
- *Begrænsning af antal autorisationsansvarlige og brugeradministratorer*
- *Centraliseret rettighedsstyring*
- *Rollebaserede adgangsrettigheder*
- *Kontrolleret/forhindret dublering af adgangsrettigheder*
- *Kontrolleret/forhindret genanvendelse af autorisation*
- *Forhindring af anonym adgang*
- *Styring af fysiske adgange*
- *Awareness*
- *Dokumentation af autorisationer*
- *Automatisk lukning af inaktive adgange*
- *Forlods angivelse af adgangslukning*

Personalemæssige ændringer i en organisation

- Når medarbejdere skifter afdeling eller får nye arbejdsopgaver og når nye medarbejdere onboardes, er der særlig grund til at være opmærksomhed ~~på~~, om adgangsrettigheder skal ændres. Dette forudsætter, at man ikke kun har fokus på oprettelse af nye adgangsrettigheder, men også nedlæggelse af de eksisterende.

[GRAFIK: person på vej ind i hus]

Relevante foranstaltninger

- *Funktionsadskillelse*
- *Styring af fysiske adgange*
- *Tilpasning af adgangsrettigheder ved ændring af ansættelse*
- *Dataadgang efter behov*
- *Adgangsrettigheder efter behov*
- *Adgang koblet til viden*
- *Minimering af privilegerede adgangsrettigheder*
- *Awarenes*

- Ved off-boarding af medarbejdere i forbindelse med fratrædelse eller afskedigelse, skal der typisk ske en lang række ting, for at sikre inddragelse af adgangsrettigheder, og hurtig inddragelse kræver normalt, at man er forberedt.

[GRAFIK: person på vej ud af hus]

Relevante foranstaltninger

- *NY: Sikre at information om fratrædelse deles til ansvarlige for brugeradministration, såfremt proceduren ikke er automatiseret*
- *Styring af fysiske adgange*
- *Tilpasning af adgangsrettigheder ved ændring af ansættelse*

Kommentar [F22]: Der bør tilføjes en dot, som formulerer behovet for information om, at fratrædelser tilflyder it-ansvarlige. Mange brugeradgange forbliver åbne efter medarbejderfratrædelse, fordi informationer ikke når frem til de, som skal udføre lukningen.

- Orlov, barsel, sygemelding mv. er situationer, der i samme grad som fratrædelse skal ske med opmærksomhed på, ~~at~~ hvilke adgangsrettigheder, der bør inddrages eller midlertidigt deaktiveres.

Kommentar [F23]: Her er det vigtigt at have fokus på, at den fortløbende dialog – og evt. adgang – er vigtig for at fastholde medarbejdere på orlov, barsel mv.. For stor rigiditet kan have negative effekter.

[GRAFIK: person sammen med timeglas udenfor hus]

Relevante foranstaltninger

- *Styring af fysiske adgange*
- *Tilpasning af adgangsrettigheder ved ændring af ansættelse*

- Ved engagering af ekstern/midlertidig arbejdskraft, fx konsulenter til softwareudvikling, vikarer, mv. er der særlige forhold, som gør sig gældende, om end det meste kan foregå efter de samme principper, som ved ansættelse af medarbejdere:

[GRAFIK: person sammen med timeglas i hus]

Relevante foranstaltninger (ud over dem som relaterer sig til normale ansættelser)

- *Forlods angivelse af adgangslukning*
- *Awareness*
- *Dataadgang efter behov*
- *Adgangsrettigheder efter behov*
- *Adgang koblet til viden*
- *Minimering af privilegerede adgangsrettigheder*

Kommentar [F24]: Vi mener, at disse foranstaltninger også bør nævnes.

Udvikling eller erhvervelse af nyt it-system eller udvikling/ændring i eksisterende it-system

Nyudvikling og erhvervelse af nye it-systemer eller væsentlige ændringer i eksisterende systemer med nye eller ændrede funktioner, kræver, at der helt fra start fokuseres på rettighedsstyring. ~~Der skal om nødvendigt udvikles/vælges på en sådan måde, at~~ Ff ølgende foranstaltninger ~~kan~~ bør overvejes ~~implementeres eller bliver~~ implementeret i it-systemet.

Kommentar [F25]: Bud på sproglig tydeliggørelse af, at der ikke er tale om en række af "skal-krav", som alle skal implementeres.

Leverandørkravene i den fællesoffentlige rammearkitektur bør indtænkes i forbindelse med nyerhvervelser eller væsentlige ændringer af it-systemer.

[GRAFIK: bits (000110110100) på vej ind i huset]

Relevante foranstaltninger

- *Funktionsadskillelse*
- *Centraliseret rettighedsstyring*

- *Rollebaserede adgangsrettigheder*
- *Styring af fysiske adgange.*
- *Dataadgang efter behov*
- *Adgangsrettigheder efter behov*
- *Logning af brugernes anvendelser af personoplysninger*
- *Logning af brugeradministrators handlinger*
- *Pseudonymisering, anonymisering*
- *Automatisk lukning af inaktive adgange*
- *Ændringsstyring (Change Management)*

Outsourcing af behandling af personoplysninger til databehandler eller aftale med ny databehandler

Hvis du overlader det til en databehandler at administrere dine it-systemer, så kan alle foranstaltningerne i kataloget potentielt være relevante. Det afhænger af, hvilke opgaver databehandleren udfører for din organisation. Krav til styring af adgangsrettigheder vil altid være relevante, og derfor er det relevant at overveje, hvilke foranstaltninger der skal kræves via databehandleraftaler eller andre kontrakter. Dette gælder særligt, hvis databehandleren skal styre adgangsrettigheder på it-systemer med personoplysninger, hvor din organisation er dataansvarlig for behandlingen af disse oplysninger.

[GRAFIK: to huse med 'handshake' imellem sig]

Hvis du lader en databehandler styre adgangsrettigheder på dine vegne, har du stadig pligt til at sikre dig, at databehandleren lever op til kravene om passende sikkerhed og dermed, at rettighedsstyringen er tilstrækkelig. Du kan læse mere om dine forpligtelser om at føre tilsyn med databehandlere i Datatilsynets vejledning herom. *[Indsæt link]*

Overvågning af rettighedsstyring

Der skal løbende følges på rettighedsstyring. Der kan let ske fejl i en travl hverdag, og det kan modvirkes af, at du med jævne mellemrum kontrollerer, at de foranstaltninger, der støtter op om din rettighedsstyring, fungerer efter hensigten.

[GRAFIK: clipboard med firkanter indeholdende 'flueben' (checkmarks)]

Relevante foranstaltninger

- *Stikprøver i log over brugernes anvendelser af personoplysninger*
- *Stikprøver i log over brugeradministrators handlinger*
- *Periodisk kontrol af adgangsrettigheders aktualitet. Kontrol skal foretages af systemejer, eller på systemejers foreskrifter.*
- *Awareness*

Kommentar [F26]: Det er vigtigt at koble kontrollen forholdsvist tæt på systemejer, eller forskrifter fra denne, da det vil sikre den nødvendige indsigt i både arbejdsopgaver og dataindsamling. Fx kan 3. dot udbygges med "Kontrol skal foretages af systemejer, eller på systemejers foreskrifter. "

Kommentar [F27]: Denne tilføjelse vil underbygge, at styring af rettigheder i systemer skal ske af den, der har bragt systemet ind i organisationen, og som dermed har det største kendskab til brug og arbejdsprocedurer forbundet med systemet.

Rettighedsstyring i den fysiske verden

For at forstå alle aspekterne i rettighedsstyring, kan man lave en analogi til den fysiske verden. Sikkerheden ved at rejse med fly kan blive kompromitteret, hvis ikke det foregår efter strikse principper. Derfor skal en person, der ønsker at gå ombord, først autoriseres til dette gennem et boardingpas.

Et boardingpas giver en meget begrænset adgang for én specifik fysisk person til ét specifikt fly på én specifik afgang. Passageren har ikke adgang til hele flyet, men kun kabinen, og har dermed ikke mulighed for at styre flyet. Autorisationen (boardingpas) er desuden tidsbegrænset.

Beskyttelse af personoplysninger kræver, at der anvendes lignende strikse principper. Her beskrives et eksempel sammenholdt med anvendelse af boardingpas:

En passagers adgang til et fly	En medarbejders adgang til persondata i et it-system
Boardingpas kan udelukkende udstedes af det respektive flyselskab.	Autorisationer kan udelukkende udstedes af en autorisationsansvarlig, f.eks. medarbejderens nærmeste leder.
Passageren får kun adgang til flyet, hvis vedkommende har et boardingpas.	Medarbejderen får kun adgang til data, hvis vedkommende er blevet autoriseret til adgangen.
Passageren får kun adgang til et specifikt fly, på en specifik afgang, der opfylder et specifikt rejsebehov.	Medarbejderen får kun adgang til specifikke data, i et specifikt it-system, hvor adgangen er nødvendig for at han/hun kan udføre sine arbejdsopgaver.
Passagerens adgang begrænses til kabinen, fordi det er nok til at opfylde rejsebehovet. Passageren får ikke en adgang, der giver mulighed for at styre flyet (cockpit).	Medarbejderen får kun adgang til at foretage den type behandling af data, som er nødvendig for at han/hun kan udføre sine arbejdsopgaver, f.eks. ved at medarbejderen kun får læseadgang, og dermed ikke kan redigere i data.
Adgang til cockpit gives ikke, fordi det indebærer særlige risici, og kræver særlig viden og erfaring.	Autorisationer gives kun, når brugeren har den rette viden og erfaring, til at undgå de særlige risici, som adgangen repræsenterer.
Passageren ekskluderes fra flyet, når det er landet, fordi det specifikke rejsebehov er ophørt.	Medarbejderen adgang til data lukkes, når den ikke længere er nødvendig for at han/hun kan udføre sine arbejdsopgaver.
Når passageren er ekskluderet fra flyet efter endt rejse, kan det udstedte boardingpas ikke genanvendes.	Når adgangen til data er lukket, kan autorisationen ikke genanvendes, hvilket sikrer, at adgangsbehov genvurderes ifm. ny autorisering.

Kommentar [F28]: Dette er tænkt som en "bagside" til vejledningen.

Kommentar [F29]: "Nærmeste leder" er oftest den forkerte til at vurdere adgange, da denne vil være interesseret i flere rettigheder for at gøre hverdagen nem for medarbejderne. Samarbejdet med systemejer skal sikres her.