Styr på rettighedsstyring

– kort fortalt



Denne korte vejledning giver et overblik over de vigtigste principper for rettighedsstyring, og hvordan I sikrer, at medarbejdere kun har adgang til de personoplysninger, de har behov for. Den bygger på Datatilsynets vejledning "Styr på rettighedsstyring" og erstatter ikke den fulde vejledning, hvor I finder uddybende forklaringer, konkrete eksempler og anbefalinger.

DATATILSYNET

1. Hvad er rettighedsstyring?

Rettighedsstyring handler om at styre, hvem der har adgang til organisationens it-systemer, oplysninger og lokaler, og hvad de enkelte personer må bruge deres adgang til.

Det er ikke tilstrækkeligt at sikre, at kun bestemte medarbejdere kan logge ind i et system. I skal også tage stilling til, hvilke oplysninger medarbejderne har behov for, og hvad de skal kunne gøre med dem.

Rettighedsstyring omfatter også fysiske adgange, f.eks. adgang til lokaler og arkiver med personoplysninger på papir.

Hvad kræver GDPR?

Efter GDPR skal dataansvarlige og databehandlere gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til risiciene ved behandlingen af personoplysninger.

Det betyder, at I skal vurdere, hvilke risici der er forbundet med behandlingen, og hvilke foranstaltninger der er nødvendige for at beskytte oplysningerne.

Rettighedsstyring er en central del af dette arbejde. De konkrete løsninger afhænger b.la. af, hvilke oplysninger I behandler, hvem der har adgang til dem, og hvilke konsekvenser det kan få, hvis uvedkommende får adgang.

2. Giv kun adgang, når der er behov for det

Medarbejdere skal kun have adgang til de personoplysninger, de har behov for til deres arbejdsopgaver. Deres rettigheder til at bruge oplysningerne skal samtidig begrænses til det nødvendige.

En medarbejder kan eksempelvis have behov for at læse oplysninger uden at skulle kunne ændre eller slette dem.

Når I tildeler adgangsrettigheder, skal I derfor tage stilling til:

- Hvilke systemer og oplysninger medarbejderen har behov for at få adgang til.
- Hvad medarbejderen skal kunne gøre med oplysningerne, f.eks. læse, ændre eller slette dem.
- Om medarbejderen har de nødvendige kompetencer til at anvende adgangen korrekt.
- Hvornår adgangen ikke længere er nødvendig.

Adgangsrettigheder bør ikke være mere omfattende end det arbejdsmæssige behov. Det gælder især rettigheder, som giver mulighed for at ændre sikkerhedsindstillinger eller få adgang til mange systemer.

EKSEMPEL

En medarbejder opretter en mappe med fortrolige HR-oplysninger på et fælles drev. Mappen bliver ved en fejl oprettet, så alle medarbejdere kan få adgang til oplysningerne.

Selv om ingen uvedkommende nødvendigvis har læst oplysningerne, er der skabt mulighed for uautoriseret adgang.

Eksemplet viser, hvorfor det er vigtigt at sikre, at adgangsbegrænsninger bliver oprettet korrekt og kontrolleret.

3. Sørg for klare ansvarsområder

God rettighedsstyring kræver, at det er klart, hvem der beslutter, tildeler og kontrollerer adgangsrettigheder.

Den autorisationsansvarlige er den person, der godkender, at en medarbejder får adgang. Det kan f.eks. være medarbejderens nærmeste leder eller den ansvarlige for et it-system.

Brugeradministratoren er den person, der tildeler eller ændrer adgangsrettigheder på baggrund af godkendelsen.

Adgangsrettigheder skal tildeles på baggrund af en godkendelse fra en person, der har kompetence til at vurdere medarbejderens behov. Godkendelsen skal bygge på medarbejderens konkrete arbejdsopgaver.

Organisationen skal have passende procedurer for, hvordan adgange administreres. Det kan blandt andet være relevant at:

- Dokumentere godkendelser af adgangsrettigheder.
- Begrænse antallet af personer, der kan godkende eller tildele adgangsrettigheder.
- Begrænse antallet af personer med særlige administratorrettigheder.
- Undgå at kopiere adgangsrettigheder fra én medarbejder til en anden uden først at vurdere behovet.
- Undgå at genbruge tidligere godkendelser uden at vurdere, om adgangen fortsat er nødvendig.

Ledelsen har ansvaret for at sikre, at organisationen arbejder aktivt med rettighedsstyring, og at der er de nødvendige procedurer og ressourcer.

Medarbejdere med ansvar for it-sikkerhed skal arbejde med at sikre, at adgangsrettigheder passer til de arbejdsmæssige behov. Alle medarbejdere bør samtidig være opmærksomme på, om deres egne adgange er relevante.

4. Tilpas adgange, når arbejdsforhold ændrer sig

Adgangsrettigheder skal ikke blot være korrekte, når de bliver tildelt. De skal også passe til medarbejderens aktuelle arbejdsopgaver. Derfor er det vigtigt at have procedurer for at ændre eller lukke adgange, når behovet ændrer sig.

Når medarbejdere får nye opgaver

Hvis en medarbejder skifter afdeling eller får nye arbejdsopgaver, skal I være opmærksomme på både at tildele eventuelle nye adgange og fjerne dem, der ikke længere er nødvendige.

En medarbejder bør ikke automatisk beholde alle tidligere rettigheder, blot fordi vedkommende fortsat er ansat i organisationen.

Når medarbejdere fratræder eller er fraværende

Ved fratrædelse skal I sikre, at medarbejderens adgange bliver lukket, når der ikke længere er behov for dem. Det kræver normalt, at I på forhånd har fastlagt, hvem der skal lukke adgangene, og hvordan det sker.

Ved orlov, barsel, sygemelding og fritstilling skal I vurdere, om medarbejderens adgange fortsat er nødvendige, eller om de bør inddrages eller midlertidigt deaktiveres.

Midlertidige medarbejdere

Vikarer, konsulenter og andre midlertidige medarbejdere skal have adgangsrettigheder, der passer til deres opgaver. Her er det særligt vigtigt at have styr på, hvornår deres adgangsbehov ophører.

EKSEMPEL

En kommune får ikke lukket adgangen til et it-system, efter at en vikar er stoppet. Vikaren kan derfor fortsat tilgå oplysninger om borgere, herunder oplysninger om deres medicin.

Den tidligere vikar misbruger adgangen, og flere borgere får efterfølgende stjålet deres medicin.

Eksemplet viser, at manglende lukning af adgangsrettigheder kan få alvorlige konsekvenser for de personer, oplysningerne handler om.

5. Tænk rettighedsstyring ind i jeres it-systemer

Rettighedsstyring bør indgå i arbejdet, når I udvikler, anskaffer eller ændrer it-systemer. Det er vigtigt at tage stilling til, hvordan adgangsrettigheder skal administreres, og hvordan I sikrer, at medarbejdere kun får adgang til de oplysninger og funktioner, de har behov for.

Afhængigt af risiciene kan det b.la. være relevant at overveje:

- **Rollebaserede adgangsrettigheder:** Adgange knyttes til bestemte arbejdsfunktioner.
- **Begrænsning af særlige rettigheder:** Antallet af medarbejdere med omfattende administrator- eller superbrugerrettigheder begrænses.
- **Logning:** Det registreres, hvordan brugere eller administratorer anvender systemerne.
- **Automatisk lukning af inaktive adgange:** Adgange, der ikke længere anvendes, kan lukkes automatisk.
- **Funktionsadskillelse:** Opgaver og rettigheder fordeles, så én person ikke unødigt kan udføre alle dele af en kritisk proces.

Det er ikke alle foranstaltninger, der nødvendigvis er relevante i enhver organisation. Valget skal bygge på en vurdering af risiciene.

Når en databehandler står for adgangen

Hvis en databehandler administrerer it-systemer eller adgangsrettigheder på jeres vegne, har I som dataansvarlig fortsat pligt til at sikre, at der er passende sikkerhed.

Det kan derfor være nødvendigt at stille krav til rettighedsstyringen i databehandleraftalen eller andre kontrakter og føre tilsyn med, at databehandleren efterlever kravene.

Databehandleren har samtidig et selvstændigt ansvar for at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger.

6. Kontrollér, at rettighedsstyringen virker

Rettighedsstyring er en løbende opgave. Selv om adgangsrettighederne er korrekte, når de bliver oprettet, kan der senere ske ændringer eller fejl, som betyder, at medarbejdere får adgang til oplysninger, de ikke længere har behov for.

I skal løbende kontrollere, om medarbejdernes adgangsrettigheder fortsat svarer til deres arbejdsopgaver, og om de foranstaltninger, I har etableret, fungerer efter hensigten.

Hvor ofte og hvordan kontrollen gennemføres, afhænger b.la. af risiciene og de fejl, kontrollen afdækker.

Det kan f.eks. ske ved at:

- Kontrollere med passende mellemrum, om medarbejdernes adgangsrettigheder fortsat er nødvendige.
- Kontrollere, at adgange bliver ændret eller lukket ved ændringer i ansættelsesforhold.
- Undersøge, om der er inaktive eller ubrugte brugerkonti, som burde være lukket.
- Sikre, at medarbejderne har den nødvendige viden til at anvende deres rettigheder korrekt.

Kontrollér også, hvordan adgangen bruges

Det er ikke altid tilstrækkeligt at kontrollere, om medarbejderne har de rigtige adgangsrettigheder. En medarbejder kan have en lovlig adgang til et system, men alligevel bruge den til at tilgå oplysninger uden et arbejdsbetinget behov.

Derfor kan det også være nødvendigt at føre løbende kontrol med medarbejdernes anvendelse af personoplysninger, f.eks. ved stikprøver i systemernes logoplysninger.

Behovet for logning og logkontrol, og hvordan kontrollen skal gennemføres, afhænger af den konkrete risikovurdering. I skal samtidig være opmærksomme på reglerne om behandling af medarbejdernes personoplysninger, herunder oplysningspligten.

Rettighedsstyring kan ikke stå alene

Det er vigtigt at være opmærksom på, at rettighedsstyring ikke kan stå alene. Et passende sikkerhedsniveau kræver ofte en kombination af tekniske og organisatoriske foranstaltninger.

Eksempelvis kan begrænsede adgangsrettigheder mindske risikoen for eller konsekvenserne af et ransomwareangreb, men de kan ikke erstatte andre nødvendige sikkerhedsforanstaltninger.

Tjekliste: Har I styr på rettighedsstyringen?

Brug spørgsmålene til at vurdere, om I har styr på de vigtigste dele af organisationens rettighedsstyring.

- ✓ Har I overblik over de systemer og personoplysninger, som medarbejderne har adgang til?
- ✓ Har I vurderet risiciene og valgt passende tekniske og organisatoriske sikkerhedsforanstaltninger?
- ✓ Har medarbejderne kun adgang til de oplysninger og funktioner, de har behov for til deres arbejdsopgaver?
- ✓ Er det klart, hvem der godkender, tildeler og ændrer adgangsrettigheder?
- ✓ Har I procedurer for at ændre eller lukke adgange, når medarbejdere skifter opgaver, fratræder eller ikke længere har behov for dem?
- ✓ Har I taget højde for rettighedsstyring ved nye eller ændrede it-systemer og ved brug af databehandlere?
- ✓ Kontrollerer I løbende, om adgangsrettighederne fortsat er nødvendige?
- ✓ Har I vurderet behovet for logning og kontrol med, hvordan medarbejderne anvender deres adgange?