Opdateret: 06.05.15

Krav om datasikkerhed i forbindelse med personaleadministration

I forbindelse med personaleadministration skal persondatalovens regler i det hele iagttages. Det indebærer bl.a., at den dataansvarlige virksomhed skal leve op til lovens krav om datasikkerhed.

Der skal træffes de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Dette følger af lovens § 41, stk. 3.

Datatilsynet har udformet nedenstående specifikke minimumskrav for sikkerhed i forbindelse med personaleadministration. Fra januar 2015 indeholder Datatilsynets tilladelser til personaleadministration i den private sektor som standard vilkår om iagttagelse af disse.

Minimumskrav for sikkerhed i forbindelse med personaleadministration:

1. Beskriv hvordan I beskytter jeres personaleoplysninger i personaleadministration og i praksis har implementeret pkt. 2-12. Beskrivelsen kan være særlige retningslinjer, der indgår i virksomhedens uddybende sikkerhedsregler, i en it-sikkerhedspolitik eller som en del af virksomhedens information til medarbejderne.

2. Adgang til oplysningerne skal begrænses til personer, der har et sagligt behov for adgang til oplysningerne. Det skal være så få personer som muligt.

3. Medarbejdere, der håndterer personaleoplysninger, skal have instruktion og oplæring i, hvad de må gøre med oplysningerne, og hvordan de skal beskytte oplysningerne.

4. Personaleoplysninger på papir – f.eks. i kartoteker og ringbind – skal opbevares aflåst, når de ikke er i brug.

   Når dokumenter (papirer, kartotekskort mv.) med personaleoplysninger skal smides ud, skal der anvendes makulering eller anden foranstaltning, der forhindrer, at uvedkommende kan få adgang til oplysningerne.

5. Der skal anvendes adgangskode for at få adgang til pc'er og andet elektronisk udstyr med personoplysninger. Kun de personer, der skal have adgang, må få en kode.

   De personer, der har adgangskode, må ikke overlade koden til andre eller lade den ligge, så andre kan se den.

   Kontrol af tildelte koder skal foretages mindst en gang hvert halve år.

6. Det skal registreres, hvis der er forgæves forsøg på at få adgang til it-systemer med følsomme personaleoplysninger. Hvis der registreres et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg, skal der blokeres for yderligere forsøg.

7. Hvis personaleoplysninger lagres på en USB-nøgle, skal oplysningerne beskyttes. Der kan f.eks. bruges en USB-nøgle med adgangskode og kryptering. Ellers skal USB-nøglen opbevares i aflåst skuffe eller skab. Tilsvarende gælder ved opbevaring af personaleoplysninger på andre bærbare datamedier.

8. PC'er koblet til internettet skal have en opdateret firewall og viruskontrol installeret.

9. Hvis der benyttes hjemmesideformularer, hvor følsomme personaleoplysninger og personnummer kan indtastes og fremsendes, skal der anvendes kryptering.

10. Hvis følsomme personaleoplysninger og personnummer sendes med e-mail via internettet, anbefaler Datatilsynet kryptering.

11. I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, og når datamedier skal sælges eller kasseres, skal der træffes de fornødne foranstaltninger, så oplysninger ikke kan komme til uvedkommendes kendskab.

12. Ved brug af en ekstern databehandler til håndtering af oplysninger, skal persondatalovens § 42 om skriftlig databehandleraftale mv. følges. Det gælder eksempelvis, når der anvendes et eksternt dokumentarkiv eller rekrutteringssystem på internettet.

Datatilsynet
Borgergade 28, 5
1300 København K
Tlf.: 33 19 32 00
Fax.: 33 19 32 18
E-mail: dt@datatilsynet.dk

Opdateret: 06.05.15

Krav om datasikkerhed i forbindelse med personaleadministration

I forbindelse med personaleadministration skal persondatalovens regler i det hele iagttages. Det indebærer bl.a., at den dataansvarlige virksomhed skal leve op til lovens krav om datasikkerhed.

Der skal træffes de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Dette følger af lovens § 41, stk. 3.

Datatilsynet har udformet nedenstående specifikke minimumskrav for sikkerhed i forbindelse med personaleadministration. Fra januar 2015 indeholder Datatilsynets tilladelser til personaleadministration i den private sektor som standard vilkår om iagttagelse af disse.

Minimumskrav for sikkerhed i forbindelse med personaleadministration:

1. Beskriv hvordan I beskytter jeres personaleoplysninger i personaleadministration og i praksis har implementeret pkt. 2-12. Beskrivelsen kan være særlige retningslinjer, der indgår i virksomhedens uddybende sikkerhedsregler, i en it-sikkerhedspolitik eller som en del af virksomhedens information til medarbejderne.

2. Adgang til oplysningerne skal begrænses til personer, der har et sagligt behov for adgang til oplysningerne. Det skal være så få personer som muligt.

3. Medarbejdere, der håndterer personaleoplysninger, skal have instruktion og oplæring i, hvad de må gøre med oplysningerne, og hvordan de skal beskytte oplysningerne.

4. Personaleoplysninger på papir – f.eks. i kartoteker og ringbind – skal opbevares aflåst, når de ikke er i brug.

   Når dokumenter (papirer, kartotekskort mv.) med personaleoplysninger skal smides ud, skal der anvendes makulering eller anden foranstaltning, der forhindrer, at uvedkommende kan få adgang til oplysningerne.

5. Der skal anvendes adgangskode for at få adgang til pc'er og andet elektronisk udstyr med personoplysninger. Kun de personer, der skal have adgang, må få en kode.

   De personer, der har adgangskode, må ikke overlade koden til andre eller lade den ligge, så andre kan se den.

   Kontrol af tildelte koder skal foretages mindst en gang hvert halve år.

6. Det skal registreres, hvis der er forgæves forsøg på at få adgang til it-systemer med følsomme personaleoplysninger. Hvis der registreres et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg, skal der blokeres for yderligere forsøg.

7. Hvis personaleoplysninger lagres på en USB-nøgle, skal oplysningerne beskyttes. Der kan f.eks. bruges en USB-nøgle med adgangskode og kryptering. Ellers skal USB-nøglen opbevares i aflåst skuffe eller skab. Tilsvarende gælder ved opbevaring af personaleoplysninger på andre bærbare datamedier.

8. PC'er koblet til internettet skal have en opdateret firewall og viruskontrol installeret.

9. Hvis der benyttes hjemmesideformularer, hvor følsomme personaleoplysninger og personnummer kan indtastes og fremsendes, skal der anvendes kryptering.

10. Hvis følsomme personaleoplysninger og personnummer sendes med e-mail via internettet, anbefaler Datatilsynet kryptering.

11. I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, og når datamedier skal sælges eller kasseres, skal der træffes de fornødne foranstaltninger, så oplysninger ikke kan komme til uvedkommendes kendskab.

12. Ved brug af en ekstern databehandler til håndtering af oplysninger, skal persondatalovens § 42 om skriftlig databehandleraftale mv. følges. Det gælder eksempelvis, når der anvendes et eksternt dokumentarkiv eller rekrutteringssystem på internettet.

Datatilsynet
Borgergade 28, 5
1300 København K
Tlf.: 33 19 32 00
Fax.: 33 19 32 18
E-mail: dt@datatilsynet.dk

Opdateret: 06.05.15

Krav om datasikkerhed i forbindelse med personaleadministration

I forbindelse med personaleadministration skal persondatalovens regler i det hele iagttages. Det indebærer bl.a., at den dataansvarlige virksomhed skal leve op til lovens krav om datasikkerhed.

Der skal træffes de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Dette følger af lovens § 41, stk. 3.

Datatilsynet har udformet nedenstående specifikke minimumskrav for sikkerhed i forbindelse med personaleadministration. Fra januar 2015 indeholder Datatilsynets tilladelser til personaleadministration i den private sektor som standard vilkår om iagttagelse af disse.

Minimumskrav for sikkerhed i forbindelse med personaleadministration:

1. Beskriv hvordan I beskytter jeres personaleoplysninger i personaleadministration og i praksis har implementeret pkt. 2-12. Beskrivelsen kan være særlige retningslinjer, der indgår i virksomhedens uddybende sikkerhedsregler, i en it-sikkerhedspolitik eller som en del af virksomhedens information til medarbejderne.

2. Adgang til oplysningerne skal begrænses til personer, der har et sagligt behov for adgang til oplysningerne. Det skal være så få personer som muligt.

3. Medarbejdere, der håndterer personaleoplysninger, skal have instruktion og oplæring i, hvad de må gøre med oplysningerne, og hvordan de skal beskytte oplysningerne.

4. Personaleoplysninger på papir – f.eks. i kartoteker og ringbind – skal opbevares aflåst, når de ikke er i brug.

   Når dokumenter (papirer, kartotekskort mv.) med personaleoplysninger skal smides ud, skal der anvendes makulering eller anden foranstaltning, der forhindrer, at uvedkommende kan få adgang til oplysningerne.

5. Der skal anvendes adgangskode for at få adgang til pc'er og andet elektronisk udstyr med personoplysninger. Kun de personer, der skal have adgang, må få en kode.

   De personer, der har adgangskode, må ikke overlade koden til andre eller lade den ligge, så andre kan se den.

   Kontrol af tildelte koder skal foretages mindst en gang hvert halve år.

6. Det skal registreres, hvis der er forgæves forsøg på at få adgang til it-systemer med følsomme personaleoplysninger. Hvis der registreres et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg, skal der blokeres for yderligere forsøg.

7. Hvis personaleoplysninger lagres på en USB-nøgle, skal oplysningerne beskyttes. Der kan f.eks. bruges en USB-nøgle med adgangskode og kryptering. Ellers skal USB-nøglen opbevares i aflåst skuffe eller skab. Tilsvarende gælder ved opbevaring af personaleoplysninger på andre bærbare datamedier.

8. PC'er koblet til internettet skal have en opdateret firewall og viruskontrol installeret.

9. Hvis der benyttes hjemmesideformularer, hvor følsomme personaleoplysninger og personnummer kan indtastes og fremsendes, skal der anvendes kryptering.

10. Hvis følsomme personaleoplysninger og personnummer sendes med e-mail via internettet, anbefaler Datatilsynet kryptering.

11. I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, og når datamedier skal sælges eller kasseres, skal der træffes de fornødne foranstaltninger, så oplysninger ikke kan komme til uvedkommendes kendskab.

12. Ved brug af en ekstern databehandler til håndtering af oplysninger, skal persondatalovens § 42 om skriftlig databehandleraftale mv. følges. Det gælder eksempelvis, når der anvendes et eksternt dokumentarkiv eller rekrutteringssystem på internettet.

Datatilsynet
Borgergade 28, 5
1300 København K
Tlf.: 33 19 32 00
Fax.: 33 19 32 18
E-mail: dt@datatilsynet.dk