Databeskyttelsespolitik for Herurecka

Overordnet organisering af personoplysninger

Herurecka ønsker som hovedregel, at anvende digitale databehandlingssystemer og digital opbevaring af personoplysninger hos eksterne leverandører, der sikkert hoster og stiller IT-systemer til rådighed, således at Herurecka ikke selv har behov for at råde over kompetence til at stå for den daglige drift drifte sådanne systemer.

Herurecka ønsker endvidere i videst muligt omfang at organisere opbevaringen af personoplysninger i bestemte centrale systemer, så personoplysninger om de enkelte personer ikke findes fordelt på flere systemer og både i elektronisk og manuel form.

1. Formål

Databeskyttelsespolitikken beskriver det ***ledelsesgodkendte niveau*** for sikkerhed i Herurecka og indeholder de overordnede sikkerhedsmålsætninger og danner grundlag for udformning af Herureckas ***I-4 datasikkerhedshåndbog*** med de underliggende retningslinjer og forretningsgange.

De retningslinjer, der udformes for at understøtte databeskyttelsespolitikkens hovedmålssætninger, skal sikre, at alle medarbejdere arbejder med og forholder sig til datasikkerhed i behandlingen af personoplysninger i det daglige arbejde.

Databeskyttelsespolitikken er især formuleret med henblik på beskyttelse af personoplysninger, men den finder tilsvarende anvendelse på økonomiske- og andre data.

Datasikkerhed er derfor en ***nøgleværdi***, og den er en naturlig del af Herureckas automatiske og manuelle databehandling af oplysninger, herunder især personoplysninger.

2. Omfang

Databeskyttelsespolitikken er gældende for alle der er tilknyttet virksomheden enten som medarbejdere, ledelse, frivilligt tilknyttede, bestyrelse, leverandører og samarbejdspartnere.

Alle ***leverandører og samarbejdspartnere***, som har fysisk eller logisk adgang til Herureckas IT-systemer, data og personoplysninger skal gøres bekendt med politikken og forpligte sig til at følge den.

Databeskyttelsespolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af Herureckas digitale databehandlingssystemer samt manuelle arkiver og registre.

3. Hovedmålsætninger og sikkerhedsniveau

Herurecka har følgende sikkerhedsmålsætning:

"Herurecka har et passende og tilstrækkeligt teknisk og organisatorisk sikkerhedsniveau, der gælder for alle ansatte, leverandører og samarbejdspartnere ved behandling af personoplysninger og andre data ved hel eller delvis anvendelsen af automatisk databehandling, samt for behandling af manuelle dokumenter."

Et passende og tilstrækkeligt databeskyttelsesniveau[1] opnås igennem tekniske og organisatoriske foranstaltninger, der sikrer:

- ***vedvarende fortrolighed, integritet, tilgængelighed og robusthed*** af Herureckas digitale behandlingssystemer og behandlingstjenester i forhold til den risikovurdering gennemføres for de enkelte systemer og personoplysninger.
- anvendelse af ***pseudonymisering og kryptering,*** hvor det er relevant, herunder ved dataudveksling med databehandlere og eksterne parter og offentlige myndigheder
- evnen til rettidigt at ***genoprette tilgængelighed*** af og adgangen til data i tilfælde af en fysisk eller teknisk hændelse
- procedurer for regelmæssig ***afprøvning, vurdering og evaluering*** af databeskyttelsessikkerheden

beskyttelse af Herureckas IT-aktiver, personoplysninger og øvrige data i Herureckas varetægt.

Et tilstrækkelige sikkerhedsniveau ***fastholdes*** ved:

- at der ***vedvarende*** forefindes ***retningslinjer og forretningsgange***, som sikrer, at datasikkerheden er en integreret del af Herureckas drift og daglige arbejde.
  Målet er, at sikre en kontinuerlig forbedringsproces, der løbende vedligeholder og optimerer databeskyttelsespolitikken, retningslinjer og forretningsgange.
- at det igennem ***kontrakt- og leverandørstyring*** sikres, at brugen af eksterne leverandører, konsulenter og samarbejdspartnere lever op til den gældende databeskyttelseslovgivning og Herureckas databeskyttelsesniveau.
- at der i forbindelse med indførelse af ***nye IT-systemer*** gennemføres:
  - passede tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er ***nødvendige*** behandles
  - hvis det skønnes nødvendigt, gennemførelse af analyse af den påtænkte behandling af personoplysningers konsekvenser for beskyttelse af oplysningerne, (***Konsekvensanalyse***)
- Herurecka følger op på datasikkerheden igennem løbende vedligeholdelse og optimering af databeskyttelsespolitikken og de dertilhørende retningslinjer og forretningsgange.

4. Organisation og ansvar

Sikkerhedsmålsætning:

[1] Som beskrevet i Databeskyttelsesforordningen artikel 32

"Alle medarbejdere har ansvar for datasikkerheden. De er bekendte med og efterlever Herureckas databeskyttelsespolitik, retningslinjer og forretningsgange, der er beskrevet i I-4 Databeskyttelseshåndbogen."

Planlægning, implementering og kontrol af datasikkerheden er defineret af Herureckas ledelse, der også er ansvarlig for implementering og vedligeholdelse af databeskyttelsessikkerhedssystemet og er ansvarlig for opfølgning på sikkerhedshændelser (brud).

Ledelse fastsætter i **I-4** Databeskyttelseshåndbogen ***hvem der har ansvaret*** for hver af institutionens, ***digitale og manuelle databehandlingssystemer***, styring af ***systemadgang og netværksadgang***, tildeling af rettigheder, indgåelse af ***IT-kontrakter og andre kontrakter***, ***indkøb af hardware og installation af software,*** behandling af ***henvendelser fra de registrerede, o***psamling og styring af ***anmeldelse af brud på persondatasikkerheden*** til Datatilsynet og de registrerede, der er berørt af bruddet

Databeskyttelsespolitikken revurderes og godkendes én gang årligt, eller i forbindelse med eventuelle situationer, der nødvendiggør det.

Ledere og medarbejdere er ansvarlige for at efterleve retningslinjer og procedurer for datasikkerhed i det daglige arbejde. Medarbejdere der konstaterer eller oplever brud på datasikkerheden skal anmelde det hurtigst muligt til nærmeste ledere eller den udpegede kontaktperson for persondata.

Den nødvendige viden og kompetence om databeskyttelse og sikkerhed kommunikeres til alle medarbejdere, og der bliver løbende arbejdet med holdninger og viden omkring databeskyttelse og sikkerhed.

Ledelsen er ansvarlig for, at databeskyttelsespolitikken overholdes.

5. Databeskyttelseshåndbogen

Databeskyttelsespolitikken uddybes af ledelsen i retningslinjer og forretningsgange. Tilsammen udgør politikken, retningslinjer, beredskabspolitik og forretningsgange Databeskyttelseshåndbogen, der inddeles i følgende hovedområder:

a) Retningslinjer for ***medarbejdernes håndtering af sikkerhed***.
   - Fokus på, at personoplysninger altid behandles fortroligt
   - Regler for login og password
   - Regler for anvendelse af mobilt udstyr, PCér, USB-nøgler, mobiltelefoner mv.
   - Regler for anvendelse af private PCér til behandling af personoplysninger vedrørende beboere og medarbejdere
   - Regler for anvendelse af internettet
   - Regler for anvendelse af mails, herunder sikker mail, og privat anvendelse af institutionens mail

- Regler for eller forbud mod download af IT-programmer, spil, billeder mv.

b) Retningslinjer for ***adgangsstyring***

c) Retningslinjer for behandling af ***data på mobile enheder***

d) Retningslinjer for anvendelse af ***sikker mail*** ved kommunikation med pårørende til beboere og klienter, kommuner og andre offentlige myndigheder

e) Retningslinjer for ***netværksstyring***, herunder trådløse netværk

f) Retningslinjer for ***styring af sikkerhedshændelser (brud)***, herunder

- Anmeldelse af sikkerhedshændelser (brud) på persondatasikkerheden til Datatilsynet og de registrerede, herunder procedurer, kontakt til databehandler og indhold i anmeldelsen
- Forretningsgange for behandling, reetablering og rettelser af personoplysninger

g) Principper og forretningsgange for ***behandling af personoplysninger*** som beskrevet nedenfor i afsnit 6

h) Retningslinjer for ***styring af IT-leverandører og databehandlere***

- Databehandleraftaler
- Databehandlerens sikkerhedsniveau og håndtering af sikkerhed

6. Principper og forretningsgange for behandling af personoplysninger

Ledelsen fastsætter principper og forretningsgange for behandling af personoplysninger, der sikrer overholdelse af Databeskyttelsesforordningen og Persondataloven.

Forretningsgangene, der ***dokumenteres***, omfatter:

- ***Principper for behandling af personoplysninger***
- Anvendelse af ***samtykke*** som grundlag for behandling af personoplysninger
- Procedurer for udøvelse af den ***registreredes rettigheder,*** herunder underretning ved registrering og udøvelse af retten til berigtigelse, sletning eller begrænsning af behandling og ret til dataportabillitet
- ***Fortegnelser udarbejdet over behandlingsaktiviteter*** med personoplysninger

7. Risikovurdering og klassifikation af data

Risikovurdering

Herurecka ønsker at være bevidst om enhver risiko, og ud fra en risikovurdering opnå et passende og tilstrækkeligt sikkerhedsniveau etableres både elektronisk og fysisk.

Ledelsen deltager aktivt i risikovurderingen og er ansvarlige for at vurdere trusler, konsekvenser og risici ved automatisk og manuel databehandling.

Det tages op i ledelsen en gang om året om risikovurderingen skal revurderes, samt ved eventuelle større ændringer i opgaver, leverandører, databehandlingssystemer.

Klassifikation

For at sikre, at systemer og data har det rigtige sikkerhedsniveau, skal disse klassificeres. Data og systemer skal klassificeres efter både tilgængelighed, integritet (pålidelighed) og fortrolighed.

Tilgængelighed
I tilgængelighedskriteriet ligger, at det skal være muligt at tilgå systemer og data for autoriserede personer, når dette er nødvendigt.

Det er for Herurecka især vigtigt med høj tilgængelighed til data og IT-systemer, der indeholder oplysninger, der anvendes i forbindelse med personoplysninger, personaleadministration, herunder lønudbetaling og indberetninger til myndigheder

Tilgængeligheden sikres først og fremmest igennem bestemmelser i de IT-kontrakter og/eller databehandleraftaler, der indgås med leverandørerne.

Integritet og pålidelighed
Med integritet og pålidelighed menes, at data om og i systemerne er korrekte, pålidelige, nøjagtige, opdaterede og fuldstændige.

Det er for Herurecka især vigtigt med høj integritet og pålidelighed i data og IT-systemer, der indeholder oplysninger, der anvendes i forbindelse med behandling af personoplysninger og personaleadministration.

Integritet og pålidelighed sikres først og fremmest gennem den kvalitetskontrol, der finder sted under de fastlagte forretningsgange for behandling personoplysninger og sager.

Fortrolighed
Med ***fortrolighed*** menes der, at kun autoriserede personer har ret til at tilgå personoplysningerne, og personoplysningerne kun skal være tilgængelige for autoriserede personer.

Personoplysninger behandles altid fortroligt og videregives eller offentliggøres kun med samtykke fra den registrerede, med mindre videregivelse har anden hjemmel i lovgivningen.

I **I-4** Databeskyttelseshåndbogen angives hvilke personer, der har adgang til henholdsvis beboernes og medarbejdernes oplysninger.

8. Overtrædelse af databeskyttelsespolitikken

Alle medarbejdere hos Herurecka er forpligtet til at efterleve den til enhver tid gældende datasikkerhedspolitik med tilhørende retningslinjer, forretningsgange og relaterede bilag.

Alle medarbejdere modtager ved deres tiltræden af stillingen en kopi af de vigtigste bestemmelser om data- og persondatasikkerhed rettet til medarbejderne.

9. Afvigelser

Hvis der opstår situationer, hvor kravene i Databeskyttelsespolitikken helt undtagelsesvist ikke kan efterleves, skal det godkendes af ledelsen og dokumenteres, og der indføres alternative sikringsforanstaltninger.

10. Udarbejdelse og ikrafttrædelse

Ændringer i sikkerhedsdokumentationen forelægges og godkendes af ledelsen.

Databeskyttelsespolitikken er godkendt den XX., og træder i kraft den XX.

Begreber og definitioner

Begreb	Definition
Fortrolighed	Kun autoriserede personer har ret til at behandle oplysningerne, der kun skal være tilgængelige for autoriserede personer.
Integritet	Det er muligt at validere, om data på systemerne er korrekte, pålidelige, nøjagtige, opdaterede og fuldstændige. Herunder sikring af Backup og eller systemdublering
Tilgængelighed	Det skal være muligt at tilgå systemer og data for autoriserede personer, når dette er nødvendigt.
Robusthed	Behandlingssystemers- og tjenesters tekniske og organisatoriske modstandsdygtighed, der beskytter dem mod skadelige hændelser. Dette kan fx være sikring mod udfald ved dublering, køling, nødstrømsanlæg, brandslukning mv.
Pseudonymisering	Behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, der opbevares separat og sikkert.
Kryptering	En proces, der omdanner de oprindelige oplysninger til oplysninger, der er ulæselig for en trediepart.
Vedvarende	Evnen til at sikre fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester er en løbende teknisk og organisatorisk forpligtelse
Databeskyttelsespolitik	Databeskyttelsespolitikken indgår i en dokumentstruktur, hvor politikken er det overordnede dokument, som besluttes af ledelsen, og som udstikker de overordnede krav og målsætninger, som opfyldes igennem specifikke retningslinjer, forretningsgange og instrukser, der findes i Databeskyttelseshåndbogen.
Retningslinjer	I retningslinjerne udfyldes de målsætninger, der er fastlagt i politikken i konkrete beskrivelser af, hvordan sikkerhedspolitikken implementeres. Retningslinjerne fungerer på et overordnet niveau og indeholder ikke tekniske og systemrelaterede beskrivelser.
Forretningsgange og instrukser	Forretningsgange og instrukser udgør specifikke vejledninger til, hvordan retningslinjerne på detaljeret niveau overholdes og implementeres i den enkelte afdeling.
Sikkerhedsforhold	Med sikkerhedsforhold menes alle de forhold, som kan påvirke oplysningers sikkerhed i forhold til fortrolighed, pålidelighed og tilgængelighed.
Sikkerhedshændelser	Begrebet forstås bredt som alle de hændelser, der påvirker databeskyttelsessikkerheden, herunder brud på sikkerheden