



Politik og procedure for persondata

1.0 Indledning

Den interne procedurebeskrivelse for persondata gælder for Grodals Regnskab IVS. Ejer Sara Grodal er ansvarlig for at regnskabsfirmaet overholder reglerne i persondataforordningen mv.

Grodals Regnskab IVS er en regnskabsvirksomhed med kunderne i fokus, som beskæftiger 3 personer. Firmaet kunder er vekslende mellem store virksomheder & små virksomheder, uden tilknytning til særlige offentlige kendte personer.

Den overordnede risiko for eksterne interesse i de persondata som opbevares/behandles vurderes som almindelig (uden forhøjet risiko).

2.0 Opbevaring af persondata

2.1 typer af Persondata

bogerholderiet indsamlet og behandler generelt følgende persondata

- Kundedata
 - Almindelige personoplysninger som navn, adresse, mail o.l.
 - Cpr.nr.
 - Bilag og regnskabsmateriale, herunder skatteoplysninger.
- Kunders medarbejderoplysninger
- Medarbejderdata herunder ansøgninger
 - Navn, adresse, Cpr.nr. og øvrige personlige oplysninger benævnt i ansøgninger.

Virksomheden opbevarer ikke flere personoplysninger end hvad der findes nødvendigt for kunne udføre samarbejdsaftalen vi har med kunden.

2.2 Opbevaring af Persondata

Vi opbevarer persondata både fysisk (papirform) og elektronisk.

Fysisk

bilag/dokumenter med persondata, herunder cpr.nr. i ringbind på virksomhedens adresser. Der arbejdes lokalt med dokumenterne i papirform på skrivebordet på virksomhedens kontoer. Bilagsmapper inkl. Persondata mellem virksomheden og kunden kan transporteres ved f.eks. arbejde hos kunder, ved modtagelse af materialer eller ved transportering til virksomhedens andet kontor.

Elektronisk

Elektronisk opbevares der persondata på virksomhedens online backup, virksomhedens adgang til bogføringsprogram, virksomhedens tidsregistreringsprogram samt virksomhedens mobiltelefoner, som alle er låste.



3.0 Risikovurdering

Fysisk

Art	Beskrivelse	Risikovurdering
<i>Fysiske rammer</i>	Virksomhedens kontor er beliggende i indehaverens privat hjem, som er beliggende i et roligt villakvarter. Der modtages til tider besøg fra kunder, potentielle kunder og samarbejdspartnere. Printer/kopimaskine er placeret ved siden af skrivebordet.	Risikoen for sikkerhedsbrud vurderes lav. Der låses til kontoret når virksomhedens medarbejdere ikke er til stede. Skrivebordet er placeret så der ikke kan ses persondata fra vinduerne, uden at indehaveren vil kunne se personen tydeligt. Samt der er vagthund på stedet.
<i>Opbevaring i ringbind</i>	På virksomhedens kontor opbevares og behandles der persondata anført på bilag, selvangivelser, lønbilag mv. i papirform, som arkiveres i ringbind.	Risikoen for sikkerhedsbrud vurderes lav. Når der ikke arbejdes med "ringbindet" står ringbind altid i på hylde i virksomhedens kontor.
<i>Arbejde på skrivebord</i>	Der arbejdes med bilag/regnskab mv. ved skrivebordet på virksomhedens kontor.	Risikoen for sikkerhedsbrud vurderes lav. Der er ikke andre på kontoret end virksomhedens medarbejdere. Ved besøg på kontoret, gemmes bilag mv. væk, således at den besøgende ikke ser øvrige kunders bilag mv.
<i>Transport</i>	Ved besøg hos kunder, hænder det at der medtages bilag mv. til/fra virksomheden til/fra kunden.	Risikoen for sikkerhedsbrud vurderes lav. Transporten sker altid i Virksomhedens medarbejders personbil. Medbragte bilag mv. opbevares i ringbind/kuverter, som endvidere ligger i en mulepose eller taske.

Elektronisk



Art	Beskrivelse	Risikovurdering
<i>Tekniske rammer - hardware</i>	Virksomhedens hardware består af bærbar PC og smartphones.	Risikoen for sikkerhedsbrud vurderes lav. Der er fornuftige login til både PC og smartphones.
<i>Tekniske rammer - software</i>	Der opbevares ingen kundedata/persondata lokalt på virksomhedens PC. Der anvendes Microsoft baseret løsning til bearbejdning og opbevaring af filer og data.	Risikoen for sikkerhedsbrud vurderes lav. Der er fornuftige login til software.
<i>Kundesystem</i>	Der bruges Visma projektstyringsprogram til oplysninger om/fra kunder. Løsningen bruger samme hosting som virksomhedens økonomisystem.	Risikoen for sikkerhedsbrud vurderes lav. Visma vurderes som et system med høj sikkerhed. Der er personlig login-adgang til systemet, som kun virksomhedens medarbejdere kender.
<i>Mailsystem</i>	Der anvendes microsoft office mail på computer samt på smartphone. Mailforsendelse sker altid ukrypteret. Der sendes mail til kunder og kunders forretningsforbindelse, med ikke-følsomme personoplysninger samt cpr.nr.	Risikoen for sikkerhedsbrud vurderes normal og acceptabel henset til scenen og ressourceforbruget ved anvendelse af krypteret mails. Virksomhedens medarbejdere er påpasselige med at mail til korrekte mailadresser. Endvidere er der fokus på at minimere antallet af mails med cpr.nr.
<i>Eget økonomisystem</i>	Virksomheden anvender e-conomic (online-system) som økonomisystem, hvori der opbevares personoplysninger på kunder, til brug for fakturering.	Risikoen for sikkerhedsbrud vurderes lav. E-conomic vurderes som et system med høj sikkerhed. Der er personlig login-adgang til systemet, som kun virksomhedens medarbejdere kender.
<i>Kundebogføring</i>	Virksomheden anvender online-økonomisystem e-conomic, hvori der	Risikoen for sikkerhedsbrud vurderes lav.



opbevares og registreres personoplysninger, på virksomhedens kunders vegne.

Der anvendes personlige login-koder. Bogføringssystemerne vurderes generelt som sikre.

4.0 Sikkerhedsbrud

Skulle der ske sikkerhedsbrud vurderes følgende:

- Arten & omfanget af sikkerhedsbruddet.
- Risikoen for at kunden kan udsættes for:
 - Id-tyveri (cpr.nr.)
 - Lide økonomisk tab
 - Tab af fortrolighed (omdømme)
 - Socialt tab

Herefter forestås der en underretning til kunden om sikkerhedsbruddet og den potentielle følge herved. Endvidere underrettet datatilsynet, medmindre forholdet vurderes at være bagatelagtigt.

5.0 Samtykkeerklæringer

Ved etablering af et kundeforhold udfærdiges der en samarbejdsaftale hvori der bl.a. indgår en samtykkeerklæring. I samtykkeerklæringen oplyses det bl.a. at vi registrere og behandler persondata og at kunden kan kræve oplysningerne slettet, dog er der krav i henhold til hvidvaskningsloven, som vi skal efterleve.

Endvidere indhentes der i kundeaftalen fuldmagt til at virksomheden kan modtage og videregive kundeoplysninger, regnskaber og andre relevante oplysninger, til kundens revisor, bankforbindelse og øvrige aktuelle samarbejdspartnere.

6.0 Virksomhedens databehandlere

Virksomhedens databehandlere består af følgende virksomheder:

Databehandlere	Beskrivelse	Aftale	Datasikkerhed
<i>E-conomic</i>	Eget økonomisystem med almindelige personoplysninger på virksomhedens kunder og kunders lønmodtagere og kunders kunder i form af bilag mv.	Ok	Sikkerheden vurderes at være på meget højt niveau og passende.
<i>Danløn</i>	Eget lønsystem med personoplysninger og cpr.nr. på	Ok	Sikkerheden vurderes at være på meget højt



	egne ansatte samt kunders ansatte.		niveau og passende.
Microsoft	Virksomhedens hostingmiljø hvor alle elektroniske dokumenter og mails opbevares.	Ok	Sikkerheden vurderes at være på højt niveau og passende.
Regnskabsfabrikanten A/S	Revisionsfirma og samarbejdspartner, som modtager kundeoplysninger ved rådgivning om kunderne.	Ok	Sikkerheden vurderes at være på højt niveau og passende.

Databehandleraftalerne er skriftlige og der opbevares en kopi heraf.

7.0 Undervisning af medarbejdere

Virksomhedens medarbejder bliver taget med til netværk møder hvor der forekommer informationer indenfor området, der er stort fokus på at medarbejdere i virksomheden er oplyste omkring emnet.

8.0 Sletning af persondata

Hvert efterår kontrolleres alle oplysninger og oplysninger der ikke længere er relevant kundedata slettes behørigt.

- Ansøgere, potentielle kunder o.l.: personoplysningerne slettes umiddelbart efter brug.
- Kunder: personoplysninger som kræves iht. Hvidvaskningsloven gemmes i 5 år efter endt kundeforhold, hvorefter de slettes. Regnskabsmateriale mv. inkl. Aktuelle personoplysninger gemmes i 5 år, hvorefter de slettes.
- Ved endt samarbejde vil originale ringbind med regnskabsmateriale, personoplysninger mv. bliver sendt med posten/afleveret til kunden.

Ved sletning gennemgås kundesystem, kundemapper, mails, og alle personoplysninger mv. slettes.

9.0 Kontrol af overholdelse af persondataforordningen

virksomhedens medarbejdere gennemgår en gang årligt (oftere hvis det skulle vurderes nødvendigt) virksomhedens procedure og politikker, herunder risikovurderinger og sikkerhedsforanstaltninger. Dette dokumenteres ved en skriftlig opsummering på gennemgang, herunder konklusion og forbedringsoversigt.