

Databehandlersaftale

Mellem

Den dataansvarlige:

[Navn]

CVR [CVR-nummer]

[Adresse]

[Postnummer og by]

[Land]

(Her efter benævnt kunden)

og

Databehandleren

Bagger Låse & Alarm A/S

CVR nr. 27920004

Ndr. Ringgade 70B

4200 Slagelse

Danmark

1 Indhold

2	Baggrund for databehandleraftalen.....	3
3	Den dataansvarliges forpligtelser og rettigheder.....	4
4	Databehandleren handler efter instruks.....	4
5	Fortrolighed	4
6	Behandlingssikkerhed.....	5
7	Anvendelse af underdatabehandlere.....	6
8	Overførsel af oplysninger til tredjelande eller internationale organisationer	7
9	Bistand til den dataansvarlige	7
10	Underretning om brud på persondatasikkerheden	9
11	Sletning og tilbagelevering af oplysninger	9
12	Tilsyn og revision	9
13	Parternes aftaler om andre forhold	10
14	Ikrafttræden og ophør.....	10
15	Kontaktpersoner/kontaktpunkter hos den dataansvarlige og databehandleren	11
Bilag A	Oplysninger om behandlingen	11
Bilag B	Betingelser for databehandlerens brug af underdatabehandlere og liste over godkendte underdatabehandlere	12
Bilag C	Instruks vedrørende behandling af personoplysninger	14
Bilag D	Parternes regulering af andre forhold.....	18

2 Baggrund for databehandleraftalen

1. Denne aftale fastsætter de rettigheder og forpligtelser, som finder anvendelse, når databehandleren foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Aftalen er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i *Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (Databeskyttelsesforordningen)*, som stiller specifikke krav til indholdet af en databehandleraftale.
3. Databehandlerens behandling af personoplysninger sker med henblik på opfyldelse af ordre, serviceaftaler og ad-hoc servicering: Servicer, supporter og installation af låse og sikringsprodukter inkl. adgangskontrol og TV-overvågning.
4. Databehandleraftalen og "ordre, serviceaftaler samt ad-hoc opgaver" er indbyrdes afhængige, og kan ikke opsiges særskilt. Databehandleraftalen kan dog – uden at opsige "ordre, serviceaftaler samt ad-hoc opgaver" – erstattes af en anden gyldig databehandleraftale.
5. Denne databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne, herunder i "ordre, serviceaftaler samt ad-hoc opgaver".
6. Til denne aftale hører fire bilag. Bilagene fungerer som en integreret del af databehandleraftalen.
7. Databehandleraftalens Bilag A indeholder nærmere oplysninger om behandlingen, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
8. Databehandleraftalens Bilag B indeholder den dataansvarliges betingelser for, at databehandleren kan gøre brug af eventuelle underdatabehandlere, samt en liste over de eventuelle underdatabehandlere, som den dataansvarlige har godkendt.
9. Databehandleraftalens Bilag C indeholder en nærmere instruks om, hvilken behandling databehandleren skal foretage på vegne af den dataansvarlige (behandlingens genstand), hvilke sikkerhedsforanstaltninger, der som minimum skal iagttages, samt hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
10. Databehandleraftalens Bilag D indeholder parternes eventuelle regulering af forhold, som ikke ellers fremgår af databehandleraftalen eller parternes "hovedaftale".
11. Databehandleraftalen med tilhørende bilag opbevares elektronisk af begge parter.

12. Denne databehandlersaftale frigør ikke databehandleren for forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt databehandleren.

3 Den dataansvarliges forpligtelser og rettigheder

1. Den dataansvarlige har overfor omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker indenfor rammerne af databeskyttelsesforordningen og databeskyttelsesloven.
2. Den dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.
3. Den dataansvarlige er blandt andet ansvarlig for, at der foreligger hjemmel til den behandling, som databehandleren instrueres i at foretage.

4 Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.
2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5 Fortrolighed

1. Databehandleren sikrer, at kun de personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den dataansvarlige. Adgangen til oplysningerne skal derfor straks lukkes ned, hvis autorisationen fratages eller udløber.
2. Der må alene autoriseres personer, for hvem det er nødvendigt at have adgang til personoplysningerne for at kunne opfylde databehandlerens forpligtelser overfor den dataansvarlige.
3. Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

4. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.

6 Behandlingssikkerhed

1. Databehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.
2. Ovenstående forpligtelse indebærer, at databehandleren skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:
 - 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
3. Databehandleren skal i forbindelse med ovenstående – i alle tilfælde – som minimum iværksætte det sikkerhedsniveau og de foranstaltninger, som er specificeret nærmere i denne aftales Bilag C.
4. Parternes eventuelle regulering/aftale om vederlæggelse eller lign. i forbindelse med den dataansvarliges eller databehandlerens efterfølgende krav om etablering af yderligere sikkerhedsforanstaltninger vil fremgå af parternes ”hovedaftale” eller af denne aftales bilag D.

7 Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2 og 4, for at gøre brug af en anden databehandler (underdatabehandler).
2. Databehandleren må således ikke gøre brug af en anden databehandler (underdatabehandler) til opfyldelse af databehandlertaften uden forudgående specifik eller generel skriftlig godkendelse fra den dataansvarlige.
3. I tilfælde af generel skriftlig godkendelse skal databehandleren underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.
4. Den dataansvarliges nærmere betingelser for databehandlerens brug af eventuelle underdatabehandlere fremgår af denne aftales Bilag B.
5. Den dataansvarliges eventuelle godkendelse af specifikke underdatabehandlere er anført i denne aftales Bilag B.
6. Når databehandleren har den dataansvarliges godkendelse til at gøre brug af en underdatabehandler, sørger databehandleren for at pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er fastsat i denne databehandlertaftale, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen.

Databehandleren er således ansvarlig for – igennem indgåelsen af en underdatabehandlertaftale – at pålægge en eventuel underdatabehandler mindst de forpligtelser, som databehandleren selv er underlagt efter databeskyttelsesreglerne og denne databehandlertaftale med tilhørende bilag.

7. Underdatabehandlertaften og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom - i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at der er indgået en gyldig aftale mellem databehandleren og underdatabehandleren. Eventuelle kommercielle vilkår, eksempelvis priser, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandlertaften, skal ikke sendes til den dataansvarlige.
8. Databehandleren skal i sin aftale med underdatabehandleren indføre den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for

underdatabehandleren, f.eks. så den dataansvarlige kan instruere underdatabehandleren om at foretage sletning eller tilbagelevering af oplysninger.

9. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

8 Overførsel af oplysninger til tredjelande eller internationale organisationer

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel (overladelse, videregivelse samt intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.
2. Uden den dataansvarliges instruks eller godkendelse kan databehandleren – indenfor rammerne af databehandleraftalen - derfor bl.a. ikke;
 - a. videregive personoplysningerne til en dataansvarlig i et tredjeland eller i en international organisation,
 - b. overlade behandlingen af personoplysninger til en underdatabehandler i et tredjeland,
 - c. lade oplysningerne behandle i en anden af databehandlerens afdelinger, som er placeret i et tredjeland.
3. Den dataansvarliges eventuelle instruks eller godkendelse af, at der foretages overførsel af personoplysninger til et tredjeland, vil fremgå af denne aftales Bilag C.

9 Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel 3.

Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

- a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
- b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede

- c. den registreredes indsigtsret
 - d. retten til berigtigelse
 - e. retten til sletning (»retten til at blive glemt«)
 - f. retten til begrænsning af behandling
 - g. underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
 - h. retten til dataportabilitet
 - i. retten til indsigelse
 - j. retten til at gøre indsigelse mod resultatet af automatiske individuelle afgørelser, herunder profilering
2. Databehandleren bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, jf. art 28, stk. 3, litra f.

Dette indebærer, at databehandleren under hensyntagen til behandlingens karakter skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

- a. forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen
 - b. forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødigt forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet, medmindre det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
 - c. forpligtelsen til – uden unødigt forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
 - d. forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
 - e. forpligtelsen til at høre tilsynsmyndigheden (Datatilsynet) inden behandling, hvis en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen
3. Parternes eventuelle regulering/aftale om vederlæggelse eller lignende i forbindelse med databehandlerens bistand til den dataansvarlige vil fremgå af parternes ”hovedaftale” eller af denne aftales bilag D.

10 Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en eventuel underdatabehandler.

Databehandlerens underretning til den dataansvarlige skal om muligt ske senest [antal timer] efter at denne er blevet bekendt med bruddet, sådan at den dataansvarlige har mulighed for at efterleve sin eventuelle forpligtelse til at anmelde bruddet til tilsynsmyndigheden indenfor 72 timer.

2. I overensstemmelse med denne aftales afsnit 10.2., litra b, skal databehandleren - under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for denne – bistå den dataansvarlige med at foretage anmeldelse af bruddet til tilsynsmyndigheden. Det kan betyde, at databehandleren bl.a. skal hjælpe med at tilvejebringe nedenstående oplysninger, som efter databeskyttelsesforordningens artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse til tilsynsmyndigheden:
 - a. Karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
 - b. Sandsynlige konsekvenser af bruddet på persondatasikkerheden
 - c. Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden, herunder hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

11 Sletning og tilbagelevering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling forpligtes databehandleren til, efter den dataansvarliges valg, at slette eller tilbagelevere alle personoplysninger til den dataansvarlige, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.

12 Tilsyn og revision

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise databehandlerens overholdelse af databeskyttelsesforordningens artikel 28 og denne aftale, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.
2. Den nærmere procedure for den dataansvarliges tilsyn med databehandleren fremgår af denne aftales Bilag C.

3. Den dataansvarliges tilsyn med eventuelle underdatabehandlere sker som udgangspunkt gennem databehandleren. Den nærmere procedure herfor fremgår af denne aftales Bilag C.
4. Databehandleren er forpligtet til at give myndigheder, der efter den til enhver tid gældende lovgivning har adgang til den dataansvarliges og databehandlerens faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13 Parternes aftaler om andre forhold

1. En eventuel (særlig) regulering af konsekvenserne af parternes misligholdelse af databehandleraftalen vil fremgå af parternes "hovedaftale" eller af denne aftales Bilag D.
2. En eventuel regulering af andre forhold mellem parterne vil fremgå af parternes "hovedaftale" eller af denne aftales Bilag D.

14 Ikrafttræden og ophør

1. Denne aftale træder i kraft ved begge parters underskrift heraf.
2. Aftalen kan af begge parter kræves genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i aftalen giver anledning hertil.
3. Parternes eventuelle regulering/aftale om vederlæggelse, betingelser eller lignende i forbindelse med ændringer af denne aftale vil fremgå af parternes "hovedaftale" eller af denne aftales bilag D.
4. Opsigelse af databehandleraftalen kan ske i henhold til de opsigelsesvilkår, inkl. opsigelsesvarsel, som fremgår af "ordre, serviceaftaler samt ad-hoc opgaver".
5. Aftalen er gældende, så længe behandlingen består. Uanset "ordre, serviceaftaler samt ad-hoc opgaver" og/eller databehandleraftalens opsigelse, vil databehandleraftalen forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos databehandleren og eventuelle underdatabehandlere.
6. Underskrift sendes via Penneo

På vegne af den dataansvarlige

Navn:

Stilling:

På vegne af databehandleren

Navn: Thomas Bagger

Stilling: Indehaver/dataansvarlig

15 Kontaktpersoner/kontaktpunkter hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner/kontaktpunkter:
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersonen/kontaktpunktet.

Navn:	Navn:	Thomas Bagger
Stilling:	Stilling:	Indehaver
Telefon-nummer:	Telefon-nummer:	70 20 21 12
E-mail:	E-mail:	bagger@bagger-laase.dk

Bilag A Oplysninger om behandlingen

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er:

TVO(videoovervågning): At detektere og registrere kriminelle handlinger samt at skabe tryghed for de ansatte. Behandling af optagelser for kunden og videregive disse til politi, advokat, forsikrings-selskaber og myndigheder på vegne af kunden.

ADK(adgangskontrol): At sikre en korrekt database over personer med adgang til virksomheden, virksomhedens bygninger, installationer og lokationer således at uønsket adgang ikke finder sted.

Behandling af database, log for kunden og videregive dette til politi, advokat, forsikringsselskaber og myndigheder på vegne af kunden.

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen):

TVO(videoovervågning): Lagring og overvågning af tv-overvågningsanlæg på de til enhver tid lokationer, adresser og kameraplaceringer kunden måtte have.

ADK(adgangskontrol): Vedligeholdelse, servicering og opdatering af databasen i forbindelse med kundens adgangskontrolsystem på de til enhver tid lokationer, adresser og adgangskontrolplaceringer kunden måtte have.

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

TVO(videoovervågning): Særlige personoplysninger jf. GDPR artikel 9 og 10

ADK(adgangskontrol): Personoplysninger, herunder særligt CPR-nummer.

Behandlingen omfatter følgende kategorier af registrerede:

TVO(videoovervågning): Medarbejdere, kunder, gæster, leverandører, fragtmænd og kriminelle (f.eks. røvere, tyve, indbrudstyve m.fl.).

ADK(adgangskontrol): Ansatte hos kunden samt kundens, leverandører, underleverandører (f.eks. håndværkere, fragtmænd, postbude, rengøring, grossister m.fl.).

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter denne aftales ikrafttræden. Behandlingen har følgende varighed:

Behandlingen er ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af parterne.

Bilag B Betingelser for databehandlerens brug af underdatabehandlere og liste over godkendte underdatabehandlere

B.0 Betingelser for databehandlerens brug af eventuelle underdatabehandlere

Databehandleren har den dataansvarliges generelle godkendelse til at gøre brug af underdatabehandlere. Databehandleren skal dog underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. En sådan underretning skal være den dataansvarlige i hænde minimum 1 måned før anvendelsen eller ændringen skal træde i kraft. Såfremt den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give meddelelse herom til databehandleren inden 7 dage efter modtagelsen af underretningen. Den dataansvarlige kan alene gøre indsigelse, såfremt den dataansvarlige har rimelige, konkrete årsager hertil.

B.1 Godkendte underdatabehandlere

Den dataansvarlige har ved databehandleraftalens ikrafttræden godkendt anvendelsen af følgende underdatabehandlere:

Navn	CVR-nr	Adresse	Beskrivelse af behandling
KeyBalance A/S	31066557	Brudelysvej 23, 2880 Bagsværd	ERP system, HR-system, dokumentering, booking og planlægningssystem, alm. persondata, økonomi, samt cpr. nr. og billeder.
Ravn IT	26406137	Snebærvej 3, 4200 Slagelse	IT-Infrastruktur, e-mail, backup, it-sikkerhed, server vedligeholdelse. Herunder alm. persondata og billeder.
Generaxion A/S	31189810	Sommervej 23A, 1. Hasle, 8210 Aarhus V	Markedsføring, nyhedsbrevssystem, administration af sociale medier, Facebook, LinkedIn, YouTube samt annoncering på sociale medier og google displaynetværk. Hjemmesiden www.bagger-laase.dk , Google My Business, Google Adwords, Google søgemaskine, Google analytics. Alm. Persondata.
VK Data ApS	28846703	Bønderbyvej 21, 6270 Tønder	Fjernstyringssoftware til pc og server.
Danske Inkasso	28891911	Munkehaten 9, 5220 Odense SØ	Økonomi og alm. persondata
Den Jyske kontrol-central	12760280	Lindevej 8, 6710 Esbjerg V	Tyverialarm/videoovervågning, Cloud løsning, alm. persondata og billeder samt videoovervågning.
Lemvig Müller	56973311	Stationsalleen 40, 2730 Herlev	Support/analyse af Videoovervågning, tyverialarm, Adgangskontrol, Cloud løsninger, alm. persondata, og billeder.
Flextrack ApS	19670546	Høgevej 19, 6705 Esbjerg Ø	Alle typer personoplysninger: Overfaldsalarm.
Ahlsell Danmark A/S	42997811	Jydenkrogen 2A, 2625 Vallensbæk	Support/analyse af Videoovervågning, tyverialarm, Adgangskontrol, Cloud løsninger, alm. persondata, og billeder.
Base Online	35853006	Gasværksvej 1B, 1.tv., 2630 Taastrup	Tidsregistrering
ARAS Security A/S	27556574	Mose Alle 10B, 2610 Rødovre	
Webaze Cloud & Låseservice	28055978	Dadevej 32, 4171 Glumsø	Cloudløsning
IT-Effect A/S	25354788	Bohrsvej 1, 8600 Silkeborg	Leverandør af Business Central og MITIT, dokumentering, booking og planlægningssystem, alm. persondata, økonomi, samt cpr. nr. og billeder.
Microsoft, herunder Business Central, Outlook, Sharepoint, Teams			ERP system, HR-system, opbevaring af e-mails, dokumentering, billeder, alm. Persondata, økonomi, cpr. nr. og billeder.
Eagle Eye Networks			Cloud baseret videoovervågning og backup.

Den dataansvarlige har ved databehandleraftalens ikrafttræden specifikt godkendt anvendelsen af ovennævnte underdatabehandlere til netop den behandling, som er beskrevet ud for parten. Databehandleren kan ikke – uden den dataansvarliges specifikke og skriftlige godkendelse – anvende den enkelte underdatabehandler til en ”anden” behandling end aftalt eller lade en anden underdatabehandler foretage den beskrevne behandling.

Bilag C Instruks vedrørende behandling af personoplysninger

C.0 Aftalens område

Denne aftale er gældende for alle aktiviteter som defineret i GDPR artikel 4 nr. 2 ”behandling”. Behandling af personoplysninger, der kræver en databehandleraftale skal fortolkes i overensstemmelse med Justitsministeriets og Datatilsynets vejledning af november 2017 ”Vejledning om dataansvarlige og databehandlere”. Det vil sige, at kun hvor formålet med selve aftalen mellem parterne angår behandling af personoplysninger og ikke en it- eller håndværksmæssig ydelse, skal der foreligge en databehandleraftale.

Nærværende aftale angår således behandling, herunder lagring af tv-overvågning (TVO) samt vedligeholdelse og inddatering af personoplysninger om ansatte i adgangskontrolanlægget (ADK). Aftale om behandling af signaler fra AIA, vil i henhold til ovennævnte vejledning ikke være omfattet af krav om en databehandleraftale, så længe personoplysninger kun behandles for at kunne identificere f.eks. kontaktpersoner hos kunden, som er nødvendige for, at sikringsleverandøren kan levere sin hovedydelse. F.eks. installation, service, opdatering eller behandling af alarmsignaler

C.1 Behandlingens genstand/ instruks

Den dataansvarlige har ansvaret for at den her omhandlede databehandling må foregå efter gældende regler og forskrifter for behandling af personoplysninger.

Databehandler, må kun behandle data efter dokumenteret instruks fra den dataansvarlige, som afgør til hvilke formål og hvordan der må foretages behandling af personoplysninger. Databehandleren eller eventuelle underdatabehandlere må derfor f.eks. ikke:

- Indsamle personoplysninger, som ligger udenfor rammerne af aftalen/instruksen
- Videregive oplysninger i et videre omfang end aftalt eller på andre måder end aftalt
- Slette oplysninger efter en anden tidsperiode end angivet af den dataansvarlige

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

TVO: Optagelserne fra tv-overvågning af de til enhver tid lokationer, adresser og kameraplaceringer kunden måtte have lagres i maksimum 30 dage.

Udenfor normal åbningstid overvåges tv-overvågningsoptagelserne ved alarm. Ved detektion af en kriminel handling eller uønsket tilstedeværelse sendes en vagt til stedet og politiet underrettes. Der er desuden i nogle tilfælde mulighed for "talk back", således at man kan tale til gerningsmanden.

Alle andre handlinger, som f.eks. videregivelse af optagelser eller lagring af billederne i mere end 30 dage, kan kun foretages efter direkte skriftlig instruks fra den dataansvarlige.

ADK: Databehandler vedligeholder databasen, der ligger til grund for adgangskontrolsystemet. Nye brugere oprettes og brugere, der har forladt kunden slettes. Data opbevares så længe det er nødvendigt, og slettes efter skriftlig meddelelse fra den dataansvarlige.

C.2 Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

"At der er tale om behandling af en stor mængde personoplysninger omfattet af databeskyttelsesforordningens artikel 9 om "særlige kategorier af personoplysninger", hvorfor der skal etableres et "højt" sikkerhedsniveau."

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe det nødvendige (og aftalte) sikkerhedsniveau omkring oplysningerne.

Databehandleren skal dog – i alle tilfælde og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige på baggrund af den risikovurdering den dataansvarlige har foretaget:

Alle medarbejdere har tavshedspligt i Bagger Låse & Alarm. Det vil sige, at den viden og information man opnår i sit arbejde om kunden ikke må videregives til 3. part. Over holdes dette ikke, vil den pågældende medarbejder som udgangspunkt blive retsforfulgt eller afskediget.

På sociale medier (f.eks. Facebook, Twitter, LinkedIn, YouTube og hjemmesider) må der ikke lægges oplysninger af nogen art om kunden. Dette gælder også statusopdateringer, chatforums og blogge.

Tavshedspligten må kun brydes ved skriftligt samtykke fra Bagger Låse & Alarm og dataansvarlige.

Fysisk sikkerhed

Der er oprettet rimelige restriktioner for fysisk adgang til Bagger Låse & Alarm A/S lokationer. Adgang til kontorlokalerne kræver aktivering af en læser via en nøglebrik, som er udleveret til Bagger Låse & Alarm A/S personale samt rengøring. Der er ligeledes installeret alarmsystemer, som kobler op til kontrolcentral i forbindelse med uberettiget adgang til lokalerne.

Områder hvor der sker behandling af personoplysninger, hvad enten det sker manuelt eller elektronisk, har passende adgangskontroller, og er effektivt adskilt fra områder, hvor der er generel adgang.

For at opnå adgang til Bagger Låse & Alarm A/S serverrum og serverskab, kræves der desuden identifikation via en adgangsbrik med log. For at opnå adgang til skabe med personoplysninger kræves der identifikation via en adgangsbrik med log.

På Bagger Låse & Alarm A/S lokationer er der opsat videoovervågning, såvel indendørs som uden-dørs, som hele tiden er aktiveret og optager på bevægelse.

Bagger Låse & Alarms lokationer i Slagelse og Ballerup er ligeledes overvåget af et røgmeldesystem som advarer mod røgudvikling. Samt temperaturovervågning af server- og teknikrum.

Teknisk sikkerhed

Bagger Låse & Alarm A/S medarbejderes enheder er sikret med antivirus samt webfilter på medarbejdernes enheder, som sørger for sikker webadgang fra og til disse, når der arbejdes udenfor Bagger Låse & Alarm A/S kontorlokaler.

Der er koder på mobiltelefoner, pc'er og øvrige enheder. Hvor det er muligt er der opsat 2-faktor validering for at opnå adgang til data på disse enheder. Der er etableret firewall, der løbende vedligeholdes. Der anvendes antivirus programmer, spam filtre og avancerede e-mailfiltre, som løbende ajourføres.

Bagger Låse & Alarm A/S holder sig, som låse- og sikringsvirksomhed, altid opdateret med henblik på at sikre den bedst mulige sikkerhed på alle dele af virksomhedens IT-systemer.

Organisatorisk sikkerhed

Kun de personer, som autoriseres hertil, har adgang til data/personoplysninger omfattet af aftalen. Medarbejdere tildeles roller/brugerrettigheder i forhold til deres arbejdsopgaver.

Autorisationer angiver i hvilket omfang brugeren må oprette, rette eller deaktivere oplysninger.

Der stilles krav om en sikker identifikation af brugerne i Bagger Låse & Alarm A/S egne IT-systemer samt en sikker metode til autorisation og kontrol af brugerrettigheder via koder og, hvor det er muligt, 2-faktor validering.

Der autoriseres kun personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere bliver ikke autoriseret til anvendelser, som de ikke har behov for.

Der kan gives autorisation til personer, for hvem adgang til oplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

Autorisationer tilbagekaldes uden ugrundet ophold, når brugeren ikke længere opfylder kriterierne for at have adgang.

Anvendte autentifikationsmekanismer lever op til, hvad der er god skik på området.

Der er procedurer for håndtering af løbende ændring af adgangskoder.

Der er procedurer for opdatering af IT-systemer.

Sletteprocedurer og procedurer ved tilbagelevering af data.

Der er en procedure for at sikre, at der sker effektiv sletning af persondata inden udstyr overgives til tredjemand eller i øvrigt bortskaffes.

C.3 Opbevaringsperiode/Sletterutine

TVO: Personoplysningerne fra tv-overvågning opbevares i 30 dage, hvorefter de slettes hos databehandleren, medmindre den dataansvarlige skriftligt anmoder om, at de gemmes længere i forbindelse med en civilretlig tvist.

ADK: Alle for opgavens løsning nødvendige personoplysninger må ikke opbevares længere end nødvendigt af hensyn til de formål hvortil de er indsamlet, herunder frister fastsat i lovgivning, og slettes senest ved opgavens afslutning eller før, hvis den dataansvarlige kræver det.

Ved samarbejdsaftalens ophør sletter eller tilbageleverer, databehandler alle data efter den dataansvarliges valg. Der må ikke gemmes kopier af data medmindre regler og love foreskriver dette.

Selvom samarbejdsaftalen mellem dataansvarlige/kunden og Bagger Låse & Alarm ophører, gælder denne instruks fortsat så længe, der behandles data hos databehandleren for den dataansvarlige.

C.4 Lokalitet for behandling

Behandling af de i aftalen omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end de følgende:

De til enhver tid lokationer, adresser, kameraplaceringer og adgangskontrolplaceringer kunden måtte have så længe aftalen er gældende.

C.5 Instruks eller godkendelse vedrørende overførsel af personoplysninger til tredjelande

Et tredjeland er et land, som ikke er medlem af EU eller EØS (Island, Liechtenstein og Norge).

I henhold til forordningens artikel 45 stk. 3 kan data uden godkendelse af Datatilsynet overføres til tredjelande der er godkendt af Kommissionen.

Hvis den dataansvarlige ikke i dette afsnit eller ved en efterfølgende skriftlig meddelelse har angivet en instruks eller godkendelse vedrørende overførsel af personoplysninger til et tredjeland, må databehandleren ikke indenfor rammerne af databehandleraftalen foretage en sådan overførsel.

C.6 Nærmere procedurer for den dataansvarliges tilsyn med den behandling, som foretages hos databehandleren

Den dataansvarlige eller en repræsentant for den dataansvarlige foretager 1 gang årligt et fysisk tilsyn vedrørende overholdelsen af denne databehandlersaftale hos databehandleren.

Udover det planlagte tilsyn, kan der føres tilsyn med databehandleren, når der efter den dataansvarliges vurdering opstår et behov herfor.

Den dataansvarliges eventuelle udgifter i forbindelse med et fysisk tilsyn afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig for, at den dataansvarlige kan gennemføre sit tilsyn.

C.7 Nærmere procedurer for tilsynet med den behandling, som foretages hos eventuelle underdatabehandlere

Databehandleren eller en repræsentant for databehandleren foretager en gang årligt et fysisk tilsyn vedrørende overholdelsen af denne databehandlersaftale hos underdatabehandleren.

Udover det planlagte tilsyn, kan der føres tilsyn med underdatabehandleren, når der efter databehandlerens (eller den dataansvarliges) vurdering opstår et behov herfor.

Dokumentation for de afholdte tilsyn sendes snarest muligt til orientering hos den dataansvarlige.”

Den dataansvarlige kan – hvis det findes nødvendigt – vælge at initiere og deltage på en fysisk inspektion hos underdatabehandleren. Dette kan blive aktuelt, såfremt den dataansvarlige vurderer, at databehandlerens tilsyn med underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker i overensstemmelse med denne databehandlersaftale.

Den dataansvarliges eventuelle deltagelse i et tilsyn hos underdatabehandleren ændrer ikke ved, at databehandleren også herefter har det fulde ansvar for underdatabehandlerens overholdelse af databeskyttelseslovgivningen og denne databehandlersaftale.

Databehandlerens og underdatabehandlerens eventuelle udgifter i forbindelse med afholdes af et fysisk tilsyn/en inspektion hos underdatabehandleren er den dataansvarlige uvedkommende – uanset at den dataansvarlige har initieret og eventuelt deltaget på et sådant tilsyn.

Bilag D Parternes regulering af andre forhold

D.0 Dokumentation

Databehandler skal stille dokumentation til rådighed for dataansvarlig, så denne kan dokumentere overholdelse af reglerne om behandling af personoplysninger, herunder GDPR og Databeskyttelsesloven samt lov om tv-overvågning.

D.1 Lovlighed

Databehandler, har pligt til uden ophold at underrette den dataansvarlige, hvis der opstår tvivl om instruksen eller databehandlingen er lovlig.

D.2 Brud på datasikkerheden

Databehandler skal uden ophold underrette den dataansvarlige om brud på datasikkerheden. Desuden skal databehandleren bistå den dataansvarlige ved en eventuel anmeldelse til Datatilsynet af brud på datasikkerheden.

D.3 Den registreredes rettigheder

Databehandler, bistår dataansvarlig med opfyldelse af pligten til at varetage de registreredes rettigheder (f.eks. ret til indsigt, berigtigelse, sletning etc. jf. GDPR artikel 12 - 22).

D.4 Fortrolighed

Databehandler, sikrer, at kun medarbejdere, der er autoriserede til at behandle personoplysninger, udfører opgaven.

Databehandler, sikrer, at de medarbejdere, der er udpeget til at behandle personoplysninger, er underlagt tavshedspligt.

D.5 Erstatning og bøder

Den dataansvarlige og/eller databehandleren kan ifalde erstatningsansvar overfor en fysisk person.

Den dataansvarlige og/eller databehandleren kan blive pålagt en administrativ bøde ved overtrædelse af forordningen eller databeskyttelsesloven.

I henhold til denne aftale kan databehandleren kun ifalde solidarisk erstatningsansvar overfor en fysisk person, hvis han har handlet i strid med instruksen fra den dataansvarlige.