

DATABASEHANDLERAFTALE

Standardkontraktsbestemmelser

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger

mellem

Haslev Privatskole
CVR 4576 8414
Jens Chr. Schous Vej 3
4690 Haslev

herefter "den dataansvarlige"

og

IST ApS
CVR 2554 5079
Gl. Marbjergvej 9
4000 Roskilde

herefter "databehandleren"

der hver især er en "part" og sammen udgør "parterne"

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

**1. Indhold**

2. Præambel	3
3. Den dataansvarliges rettigheder og forpligtelser	3
4. Databehandleren handler efter instruks	4
5. Fortrolighed	4
6. Behandlingssikkerhed	4
7. Anvendelse af underdatabehandlere	5
8. Overførsel til tredjelande eller internationale organisationer	6
9. Bistand til den dataansvarlige	7
10. Underretning om brud på persondatasikkerheden	8
11. Sletning og returnering af oplysninger	8
12. Revision, herunder inspektion	9
13. Parternes aftale om andre forhold	9
14. Ikrafttræden og ophør	9
15. Kontaktpersoner hos den dataansvarlige og databehandleren	10
Bilag A Oplysninger om behandlingen	11
Bilag B Underdatabehandlere	14
Bilag C Instruks vedrørende behandling af personoplysninger	16
Bilag D Parternes regulering af andre forhold	22

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Disse bestemmelser 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).
3. I forbindelse med leveringen af IST Tjenestetid (TRIO), behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes¹ nationale ret og disse Bestemmelser.

¹ Henvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvisning til "EØS medlemsstater".

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, 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. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.
2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.
2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

- 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.
2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.
3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.
3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 45 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandlersaftale(r) 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 tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandlersaftalen, skal ikke sendes til den dataansvarlige.
6. 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 underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.
7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.
2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.
3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:
 - a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation

- b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
 - c. behandle personoplysningerne i et tredjeland
4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.
5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

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 III.

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. indsigtssretten
 - d. retten til berigtigelse
 - e. retten til sletning ("retten til at blive glemt")
 - f. retten til begrænsning af behandling
 - g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
 - h. retten til dataportabilitet
 - i. retten til indsigelse
 - j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:
 - a. den dataansvarliges forpligtelse til uden unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
 - b. den dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis

vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

- c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
 - d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt 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. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 48 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.
3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:
 - 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. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
 - c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.
4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på

vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

12. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, 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. Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

5. Underskrift

På vegne af den dataansvarlige

Navn Gitte F. Kehl
 Stilling Skoleleder
 Telefonnummer 5631 2969
 E-mail gfk@haslevprivatskole.dk
 Underskrift 

På vegne af databehandleren

Navn Jens Arne Madsen
 Stilling Vicedirektør
 Telefonnummer 4676 1855
 E-mail jens.ame.madsen@ist.com
 Underskrift 

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Haslev Privatskole

Navn Gitte F. Kehl
 Stilling Skoleleder
 Telefonnummer 5631 2969
 E-mail gfk@haslevprivatskole.dk

Databehandleren

Navn Bettina Sudergaard
 Stilling Salgs- og marketingschef
 Telefonnummer 4676 1817
 E-mail privacy@ist.com

A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige***IST Tjenestetid***

Administrering af personales arbejdstid og opgaver. IST Tjenestetid giver mulighed for at overblik over skolens personalemæssige ressourcer.

IST Elevadministration

Formålet med behandlingen er dækning af alle administrative opgaver i grundskolen i relation til elever, lærer, klasser og hold. Det holder styr på elevernes fulde skole- og adressehistorik, holdtilmeldinger, kontaktinformation, SFO-tilmeldinger og transport mv.

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)***IST Tjenestetid***

Behandlingen hjælper skolens ledelse og administration med at planlægge skolens ressourcer, og administrerer skolen på nemmeste måde i henhold til læreraftalerne.

IST Elevadministration

Systemet dækker alle administrative opgaver, som også inkluderer indskrivning og udmelding af elever, fraværsregistrering, prøveafvikling, karaktergivning, registrering af henvisninger og specialundervisning, mellemkommunale afregninger og en række andre opgaver.



A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Side 12 af 22

IST Tjenestetid

- 1) Medarbejdere
 - a. Almindelige personoplysninger, jf. Databeskyttelsesforordningens artikel 6
 - i. Navn, telefonnummer og adresse, sygedage
 - b. Oplysninger om CPR-nummer, jf. Databeskyttelsesforordningens artikel 87

IST Elevadministration

- 1) Børn tilknyttet institutioner og skoler hos den dataansvarlige
 - a. Almindelige personoplysninger, jf. Databeskyttelsesforordningens artikel 6
 - i. Navn, telefonnummer og adresse, sygedage, billede, e-mail.
 - b. Særlige kategorier af personoplysninger, jf. Databeskyttelsesforordningens artikel 9
 - i. Racemæssig eller etnisk baggrund
 - c. Oplysninger om CPR-nummer, jf. Databeskyttelsesforordningens artikel 87
 - 2) Forældre til børn tilknyttet institutioner og skoler i Faxe Kommune
 - a. Almindelige personoplysninger, jf. Databeskyttelsesforordningens artikel 6
 - i. Navn, telefonnummer og adresse sygedage, billede, e-mail.
 - b. Særlige kategorier af personoplysninger, jf. Databeskyttelsesforordningens artikel 9
 - i. Racemæssig eller etnisk baggrund
- Oplysninger om CPR-nummer, jf. Databeskyttelsesforordningens artikel 87

A.4. Behandlingen omfatter følgende kategorier af registrerede

IST Tjenestetid

Medarbejdere

IST Elevadministration

- 1) Børn tilknyttet institutioner og skoler hos den dataansvarlige
- 2) Forældre til børn tilknyttet institutioner og skoler hos den dataansvarlige



A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Side 13 af 22

Behandlingens varighed følger aftalens længde for løsningen, der er omfattet af nærværende DBA.

B.1. Godkendte underdatabehandlere
IST Tjenestetid

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
IST Group AB	Reg.No. 556254-0806	Ingelstadsvägen 9 352 34 Växjö	IST ApS er en koncernselskab af IST Group og anvender IST Groups Private cloud setup placeret hos Interaction.

IST Elevadministration

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Onlinecity.io ApS	27364276	Buchwaldsgade 50, DK-5000 Odense C	OnlineCity.io benyttes som leverandør til afsendelse og modtagelse af sms'er
IST Group AB	Reg.No. 556254-0806	Ingelstadsvägen 9 352 34 Växjö	IST ApS er en koncernselskab af IST Group og anvender IST Groups Private cloud setup placeret hos Interaction.

Data der udveksles med Onlinecity.io

- Afsendertelefonnummer
- Modtagertelefonnummer
- Afsendernavn
- Adgangskode
- Bookingoplysninger
- Købshistorik
- E-mailadresse
- Brugernavn
- Besked indhold

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

B.2. Varsel for godkendelse af underdatabehandlere

Som beskrevet i afsnit 7, 3 skal databehandleren give et varsel på mindst 45 dage.

C.1. Behandlingens genstand/instruks

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

Instruks

Kommunen instruerer hermed Leverandøren om at foretage behandling af Kommunens oplysninger til brug for drift af løsninger, jf. hovedaftalens pkt. 2.3.

- IST Tjenestetid (TRIO)
- IST Elevadministration (TEA)

Overlader Leverandøren behandling af Kommunens oplysninger til underdatabehandlere, er Leverandøren ansvarlig for at indgå skriftlige (under)databehandleraftaler med disse. Leverandøren er ansvarlig for, at Kommunens instruks fremsendes til eventuelle underdatabehandlere.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

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

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

1. Indledning

Dette bilag indeholder en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Leverandøren i medfør af Aftalen har ansvar for at gennemføre, overholde og sikre overholdelse af hos dennes underdatabehandlere, som er angivet i bilag B.

2. Sikkerhedskrav

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, jf. Instruks (bilag A), og som dermed opfylder Databeskyttelsesforordningens artikel 32

Foranstaltningerne gennemføres for at undgå, at personoplysninger:

- I. tilintetgøres, mistes, ændres eller forringes,
- II. kommer til uvedkommendes kendskab eller misbruges,
- III. eller i øvrigt behandles i strid med lovgivningen, jf. Aftalens pkt. 2.1/2.2

Foranstaltningerne fastlægges ud fra overvejelser om:

1. Hvad der kan lade sig gøre rent teknisk
2. Implementeringsomkostningerne
3. Den pågældende behandlings karakter, omfang, sammenhæng og formål, jf. Instruksen (bilag A)
4. Konsekvenserne for borgerne ved et sikkerhedsbrud
5. Den risiko, der er forbundet med behandlingerne, herunder risikoen for:
 - a. tilintetgørelse af oplysningerne
 - b. tab af oplysningerne

- c. ændring af oplysningerne
- d. uautoriseret videregivelse af oplysningerne
- e. uautoriseret adgang til oplysningerne

IST ApS arbejder med kontinuerlige forbedringer af såvel de tekniske og organisatoriske forhold omkring persondatabehandling. Vi går til denne opgave med åbenhed, og vil gerne samarbejde med den Dataansvarlige i forhold til at finde gode løsninger på de fælles udfordringer der møder os. På nuværende tidspunkt arbejder IST aktivt med følgende områder:

- Fortegnelser over kategorier af persondatabehandlinger (Art. 30. Stk. 2.)
- Dataflowbeskrivelser,
- Udvikle gode procedure til brug for Databehandlerens bidrag til den dataansvarliges overholdelse af Persondataforordningens artikel 32 – 36, samt artikel 34 retten til indsigt

Generelle sikkerhedsforanstaltninger

IST ApS har tilrettelagt formaliserede processer, som sikrer at de organisatoriske forhold understøtter sikkerhedsforanstaltningerne i Databeskyttelseslovgivningen.

Ved indgåelse af aftaler med eksterne parter sikres den fornødne information om it-sikkerhedsmæssige krav, indgåelse af tavshedserklæringer o.l.

Ovenstående er en del af Leverandørens ISMS, der samlet set beskriver IT politik, regler og procedure for håndtering af informationssikkerheden i virksomheden.

Nye medarbejdere/eksterne konsulenter gennemgår et introduktionsforløb omhandlende informationssikkerhed, herunder leverandørens rolle som databehandler, og deraf følgende instrukser. Medarbejderen underskriver at have modtaget denne instruks.

Teknisk it sikkerhed

Ønsker kommunen en detaljeret beskrivelse af driftsmiljøets tekniske opsætning kan en sådan rekvireres ved henvendelse til Leverandøren.

IT revision af kontrolområder

Nedenstående beskrivelser af hvordan leverandøren overholder kravene i hhv. Databeskyttelsesloven og persondataforordningen, er netop genstand for årlig revision. Der foretages en årlig ekstern it revision og resultatet formidles i form af en anerkendt revisionsrapport. Den gældende erklæring er tilgængelig via leverandørens hjemmeside.

Autorisation og adgangskontrol

IST ApS har tilrettelagt kontroller til sikring af fysisk sikkerhed. Disse kontroller omfatter en række adgangskontroller i bygninger, hvor der behandles personoplysninger (adgangskort og adgangskode). Ved indgåelse af aftaler med eksterne parter sikres det, at den eksterne part modtager den fornødne information om de it-sikkerhedsmæssige krav.

IST ApS har tilrettelagt foranstaltninger for logisk sikkerhed, herunder logning og kontrol af afviste adgangsforsøg.

Disse kontroller omfatter:

- Kvalitetskrav til password
- Kontrol af afviste adgangsforsøg
- Log og opfølgning over afviste adgangsforsøg

IST ApS har tilrettelagt processer for administration af, og kontrol med, interne autorisationer. Alle interne autorisationer godkendes af medarbejdernes nærmeste chef.

IST ApS har tilrettelagt formaliserede processer, som sikrer, at tildelte brugeradgange er i overensstemmelse med arbejdsmæssigt betingede behov. Alle autorisationer godkendes af medarbejdernes nærmeste chef og indeholder begrundelse for den ønskede adgang til applikation og tilhørende data.

IST ApS har tilrettelagt formaliserede processer, som sikrer, at egne autorisationer revurderes mindst én gang hvert halve år. For så vidt angår autorisationer til produktionsmiljøet udstedes disse for en begrænset periode, og der kræves nye autorisationer ved forlængelse.

Inddatamateriale som indeholder personoplysninger

Behandling af inddata foregår via autoriserede brugers databehandling i systemet. Der foregår automatisk inddatering af grundlæggende personoplysninger fra CPR. For en beskrivelse af dette dataflow henvises til leverandørens beskrivelse "Dataflow for persondata i IST systemer".

Uddatamateriale som indeholder personoplysninger

For uddata håndteret af systemets autoriserede brugere, henvises til kommunens Informationssikkerhedsregler for håndtering af udskrifter og dataudtræk.

Backups af databaser opbevares på to fysisk adskilte lokationer og opbevares i krypteret filer på diske.

Der er mulighed for tilkøb af et "Ekstrakt" modul, der håndterer forskellige snitflader til elektronisk udtræk af data fra systemet. Brugerstyring, konfiguration og logning foretages via et administrationsinterface. Al datatransmission sker via gældende standardprotokoller og krypteringsalgoritmer.

IST ApS har udarbejdet retningslinjer for bortskaffelse, salg, kassation, reparation og service af it-udstyr indeholdende persondata.

Eksterne kommunikationsforbindelser

IST ApS har udarbejdet retningslinjer for sikring af eksterne kommunikationslinjer, og har tilrettelagt formaliserede processer, som sikrer, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

Disse kontroller omfatter:

- Retningslinjer for netværksadgang
- Kryptering af kommunikationslinjer

Systemets datatransport mellem browser og server foregår via standardiserede og gældende protokoller og krypteringsalgoritmer.

Kontrol med afviste adgangsforsøg

IST ApS har tilrettelagt foranstaltninger for logisk sikkerhed, herunder logning og kontrol af afviste adgangsforsøg.

Disse kontroller omfatter:

- Kvalitetskrav til password
- Kontrol af afviste adgangsforsøg

- Log og opfølgning over afviste adgangsforsøg.

Logning

IST ApS har tilrettelagt en række formaliserede processer vedr. logning i de tilbudte it services. Systemerne kan have forskellige typer af logs og logningsniveau. Der logges som minimum:

- Bruger login logs
- Applikations specifik log
- Brugers behandling af særlige kategorier af oplysninger/fortrolige data

Der er etableret adgangsstyring til logs. Loggen opbevares i højst 6 måneder, hvorefter den destrueres.

Alle medarbejderes adgang til systemerne logges med de nødvendige oplysninger om, hvilken bruger der har tilgået systemet, samt hvilke personer der er tilgået.

Stikprøvekontrol af brugernes systemanvendelse.

Der er mulighed for brug af fritekstfelter, hvorfor Leverandøren henholder sig til at det er kommunens ansvar at oplyse retningslinjer til medarbejderen om håndtering af personfølsomme/fortrolige oplysninger netop i fritekstfelter.

Hjemmearbejdspladser

Leverandørens behandler ikke personoplysninger fra hjemmearbejdspladser.

IST ApS har udarbejdet retningslinjer for overholdelse af sikkerhedsreglerne i forbindelse med anvendelse af Ad Hoc arbejdspladser.

Disse kontroller omfatter:

- Krav til opkobling via en sikker VPN-forbindelse
- Forbud mod at etablere andre kommunikationsforbindelser på pc'en
- Retningslinjer for behandling af data, herunder forbud mod at gemme data lokalt
- Den enkelte medarbejder bekræfter i den årlige sikkerhedserklæring, at ovenstående retningslinjer overholdes.

Hertil skal det bemærkes, at leverandøren ikke opererer med decideret fastopkoblede hjemmearbejdspladser. Medarbejdere der har behov for at arbejde i "marken" herunder i hjemmet, har mulighed for opkobling via vpn til kontor og produktionsmiljø jf. retningslinjer.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

I tilfælde af, at Kommunen og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en inspektion af de ovennævnte foranstaltninger i henhold til denne aftale, forpligter Leverandøren og Leverandørens underleverandører sig til at stille tid og ressourcer til rådighed herfor. Leverandøren forbeholder sig ret til, på vegne af Leverandøren og dennes underleverandører, at fakturere Kommunen for dokumenteret forbrugt tid, der relaterer sig til opgaver jf. nærværende afsnit. Dog er almindelig opfølgning på revisionserklæringen vederlagsfri. Timesatsen følger Leverandørens og eventuelle underleverandørers gældende timesatser. Hvis tilsynet udspringer af et brud hos leverandøren/underleverandøren er tilsynet vederlagsfrit

Som følge af pkt. 11.1 sker følgende ved ophør.

Kommunen træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af Hovedaftalen.

Kommunen skal senest 30 dage inden Hovedaftalens ophør skriftligt meddele Leverandøren, hvorvidt alle personoplysningerne skal slettes eller tilbageleveres til Kommunen. I begge tilfælde skal Leverandøren ligeledes slette eventuelle kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne. Leverandøren skal sikre, at eventuelle underdata-behandlere ligeledes efterlever Kommunens meddelelse.

Leverandøren skal fremsende dokumentation for, at den påkrævede sletning er foretaget.

Leverandøren skal foretage den påkrævede sletning i henhold til etablerede internationale standard for sletning, f.eks. NIST 800-88.

C.5 Lokaltet for behandling

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

Der henvises til Bilag B1.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Ikke relevant.

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Databehandleren skal årligt for egen regning indhente en revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionserklæringer kan anvendes i overensstemmelse med disse Bestemmelser:

- ISAE 3000 for behandling af personoplysninger og en ISAE3402- generelle It-kontroller.

Dette sker ved at revisionserklæringen lægges på IST's hjemmeside. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny revisionserklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der

benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

Databehandleren skal årligt for egen regning indhente en revisionserklæring eller inspektionsrapport fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionserklæringer eller inspektionsrapporter kan anvendes i overensstemmelse med disse bestemmelser:

- ISAE 3000 for behandling af personoplysninger og en ISAE3402- generelle It-kontroller eller dokumenteret inspektionsrapport

Dette sker ved at revisionserklæringen lægges på IST's hjemmeside. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen eller rapporten og kan i sådanne tilfælde anmode om en ny revisionserklæring eller inspektionsrapporter under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen eller rapporten er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Databehandleren eller en repræsentant for databehandleren har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når databehandleren (eller den dataansvarlige) finder det nødvendigt.

Dokumentation for sådanne inspektioner fremsendes uden unødigt forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode.

