SWECO

DATABEHANDLERAFTALER

MELLEM

FREDENSBORG FORSYNING OG SWECO DANMARK A/S OM

RENOWEB

DATABEHANDLERAFTALE

Mellem
Fredensborg Forsyning
Højvangen 23
3480 Fredensborg

CVR. nr.: 32265766
(herefter "Kunden")

og
Sweco Danmark a/s
Granskoven 8
2600 Glostrup
CVR. nr.: 48233511
(herefter "Leverandør/Databehandler")

er der indgået nedenstående databehandleraftale (herefter "Aftalen") om Leverandørens behandling af personoplysninger på vegne af Kunden i systemet RenoWeb.

1. Generelt

1.1 Aftalen vedrører Leverandørens forpligtelse til at efterleve de sikkerhedskrav, som fremgår af Lov nr. 429 af 31/05/2000 med senere ændringer om behandling af personoplysninger (Persondataloven) § 42, jf. § 41, stk. 3-5. Kravene er beskrevet i:

(i) Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsbekendtgørelsen).

(ii) Vejledning nr. 37 af 02/04/2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsvejledningen).

1.2 Den 25. maj 2018 erstattes Persondataloven af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen) således, at Aftalens pkt. 1.1 (i) – (ii) herefter erstattes med Databeskyttelsesforordningen.

1.3 I Aftalen er indarbejdet de krav, som såvel Persondataloven som de kommende regler i Databeskyttelsesforordningen stiller til databehandleraftaler.

1.4 Leverandøren skal behandle personoplysninger i overensstemmelse med god databehandlingsskik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

2. Formål

2.1 Leverandøren behandler i medfør af aftale med Kunden jf. "RenoWeb 2.0 – Aftalegrundlag, dateret 13. oktober 2009" (herefter "Hovedaftalen") personoplysninger for Kunden, hvor Leverandørens behandlinger og formålet med behandlingerne er beskrevet.

3. Kundens rettigheder og forpligtelser

3.1 Kunden er dataansvarlig for de personoplysninger, som Kunden instruerer Leverandøren om at behandle. Kunden har ansvaret for, at de personoplysninger, som Kunden instruerer Leverandøren om at behandle, må behandles af Leverandøren, herunder at behandlingen er nødvendig og saglig i forhold til Kundens opgavevaretagelse.

3.2 Kunden har de rettigheder og forpligtelser, som er givet en dataansvarlig i medfør af lovgivningen, jf. Aftalens pkt. 1.1 og 1.2.

4. Leverandørens forpligtelser

4.1 Leverandøren er databehandler for de personoplysninger, som Leverandøren behandler på vegne af Kunden, jf. pkt. 6 og bilag 3. Leverandøren har som databehandler de forpligtelser, som er pålagt en databehandler i medfør af lovgivningen, jf. Aftalens pkt. 1.1 og 1.2.

4.2 Leverandøren behandler alene de overladte personoplysninger efter instruks fra Kunden, jf. pkt. 6 og bilag 3, og alene med henblik på opfyldelse af Hovedaftalen.

4.3 Leverandøren skal fra 25. maj 2018 løbende føre en fortegnelse over behandlingen af personoplysninger samt en fortegnelse over alle sikkerhedsbrud.

4.4 Leverandøren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, som beskrevet i Sikkerhedsbekendtgørelsen og Sikkerhedsvejledningen (frem til 25. maj 2018) og Databeskyttelsesforordningen (fra 25. maj 2018), jf. bilag 1 – Sikkerhed.

4.5 Leverandøren skal på opfordring fra Kunden hjælpe med at opfylde Kundens forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra borgere om indsigt i egne oplysninger, udlevering af borgerens oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af borgerens oplysninger, samt Kundens forpligtelser i forhold til underretning af den registrerede ved sikkerhedsbrud, fra 25. maj 2018 i medfør af Databeskyttelsesforordningens kap. III samt artikel 34.

4.6 Leverandøren skal fra 25. maj 2018 hjælpe Kunden med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36.

4.7 Leverandøren garanterer fra 25. maj 2018 at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Leverandørens behandling af Kundens personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

4.8 Leverandøren er forpligtet til at oplyse med præcise adresseangivelser, hvor Kundens personoplysninger opbevares, jf. bilag 2. Leverandøren skal ajourføre oplysningerne over for Kunden ved enhver ændring.

4.9 Hvis Leverandøren er etableret i en anden EU-medlemsstat, skal Leverandøren frem til 25. maj 2018 ligeledes overholde de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat.

5. Underleverandør (underdatabehandler)

5.1 Ved underdatabehandler forstås en underleverandør, til hvem Leverandøren har overladt hele eller dele af den behandling, som Leverandøren foretager på vegne af Kunden.

5.2 Leverandøren må ikke uden udtrykkelig skriftlig godkendelse fra Kunden anvende andre underdatabehandlere end dem, der er angivet i bilag 2, herunder foretage udskiftning af disse, til at behandle de personoplysninger, som Kunden har overladt til Leverandøren i medfør af Hovedaftalen. Kunden kan ikke nægte at godkende tilføjelse eller udskiftning af en underdatabehandler medmindre, der foreligger en konkret saglig begrundelse herfor. Undtaget herfor er dog skift af leverandør af hostingmiljøet. Leverandøren må godt uden udtrykkelig skriftlig godkendelse fra Kunden skifte til en anden leverandør af hostingmiljøet, såfremt den nye leverandør også er placeret i Danmark og kan påvise revisorerklæring på overholdelse af gældende lovgivning. Hvis Kunden ikke kan acceptere Leverandørens nye hostingleverandør, er Kunden berettiget til at opsige Hovedaftalen med 3 måneds varsel til den 1. i en måned fra det tidspunkt, hvor Leverandøren overgår til den nye hostingleverandør. Leverandøren skal ajourføre oplysningerne om underdatabehandlere i bilag 2 ved enhver ændring.

5.3 Hvis Leverandøren overlader behandlingen af personoplysninger, som Kunden er dataansvarlig for, til underdatabehandlere, skal Leverandøren indgå en skriftlig (under)databehandleraftale med underdatabehandleren.

5.4 Underdatabehandleraftalen, jf. pkt. 5.3, skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som Leverandøren er pålagt efter Aftalen, herunder, at underdatabehandleren fra 25. maj 2018 garanterer at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de passende tekniske og organisatoriske foranstaltninger således, at underdatabehandlerens behandling opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

5.5 Når Leverandøren overlader behandlingen af personoplysninger, som Kunden er dataansvarlig for, til underdatabehandlere, har Leverandøren over for Kunden ansvaret for underdatabehandlernes overholdelse af disses forpligtelser, jf. pkt. 5.3.

5.6 Kunden kan til enhver tid forlange dokumentation fra Leverandøren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som Leverandøren anvender i forbindelse med opfyldelsen af sine forpligtelser over for Kunden.

5.7 Al kommunikation mellem Kunden og underdatabehandleren sker via Leverandøren.

6. Instrukser

6.1 Leverandørens behandling af personoplysninger på vegne af Kunden sker udelukkende efter dokumenteret instruks, jf. bilag 3. Det er Leverandørens ansvar at sikre, at eventuelle underdatabehandlere, jf. pkt 5.3, får tilsendt Kundens instruks, jf. bilag 3.

6.2 Leverandøren giver fra 25. maj 2018 omgående besked til Kunden, hvis en instruks efter Leverandørens vurdering er i strid med lovgivningen, jf. pkt. 1.2.

6.3 Uanset ovenstående kan Leverandøren foretage rimelige daglige handlinger med data i forbindelse med sikring af hosting og drift uden at have modtaget specifikke dokumenterede instruktioner fra Kunden, forudsat at Leverandøren handler for og med hensyn til de formål, der er angivet i bilag 3.

7. Tekniske og organisatoriske sikkerhedsforanstaltninger

7.1 Leverandøren skal frem til 25. maj 2018, jf. bilag 1, træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger:

(i) tilintetgøres, mistes, ændres eller forringes,
(ii) kommer til uvedkommendes kendskab eller misbruges, eller
(iii) i øvrigt behandles i strid med lovgivningen, jf. pkt. 1.1

7.2 Leverandøren skal fra 25. maj 2018, jf. bilag 1, iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.

7.3 Leverandøren skal 1 gang årligt gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandlingen af personoplysninger med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed er iagttaget, jf. pkt. 7.1 og 7.2, samt bilag 1.

7.4 Leverandøren samt dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.

7.5 Leverandøren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af Kundens personoplysninger, om Leverandørens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. pkt 9.

7.6 Leverandøren er forpligtet til straks at underrette Kunden om ethvert sikkerhedsbrud samt ved

(i) enhver anmodning om videregivelse af personoplysninger omfattet af Aftalen fra en myndighed, medmindre orienteringen af Kunden er eksplicit forbudt ved lov, f.eks. i medfør af regler, der har til formål at sikre fortroligheden af en retshåndhævende myndigheds efterforskning,

(ii) anden manglende overholdelse af Leverandørens, samt eventuelle underdatabehandleres forpligtelser

uanset, om dette sker hos Leverandøren eller hos en underdatabehandler.

7.7 Leverandøren må ikke hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud, jf. pkt 7.6, uden forudgående skriftlig aftale med Kunden om indholdet af en sådan kommunikation, medmindre Leverandøren har en retlig forpligtelse til sådan kommunikation.

8. Overførsler til andre lande

8.1 Leverandørens overførsel af personoplysninger til lande, der ikke er medlem af EU (tredjelande), f.eks. via en cloudløsning eller en underdatabehandler, skal ske i overensstemmelse med Kundens instruks herfor, jf. bilag 3.

8.2 Ved overførsel til tredjelande er Leverandøren og Kunden i fællesskab ansvarlige for, at der foreligger et gyldigt overførselsgrundlag.

8.3 Hvis Kundens personoplysninger overføres til en EU-medlemsstat, er det frem til 25. maj 2018 Leverandørens ansvar, at de til enhver tid gældende bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat, overholdes.

9. Tavshedspligt og fortrolighed

9.1 Leverandøren er - under og efter Hovedaftalens ophør - pålagt fuld tavshedspligt omkring alle oplysninger, denne bliver bekendt med gennem samarbejdet. Aftalen indebærer, at tavshedspligtsbestemmelserne i straffelovens §§ 152-152f, jf. straffelovens § 152a, finder anvendelse.

9.2 Leverandøren skal sikre, at alle, der behandler oplysninger omfattet af Aftalen, herunder ansatte, tredjeparter (f.eks. en reparatør) og underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

10. Kontroller og erklæringer

10.1 Leverandøren er forpligtet til at give Kunden nødvendige oplysninger til, at Kunden kan sikre sig, at Leverandøren overholder de krav, der følger af denne Aftale. Leverandørens tid honoreres i henhold til Hovedaftalen.

10.2 Kunden, en repræsentant for Kunden eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos Leverandøren, få udleveret dokumentation, herunder logs, stille spørgsmål m.v. med henblik på at konstatere, at Leverandøren overholder de krav, der følger af denne Aftale. Leverandørens tid i forbindelse med inspektioner honoreres i henhold til Hovedaftalen. I det omfang, der i forbindelse med inspektionen måtte blive konstateret problematiske

forhold vedrørende Leverandørens ansvarsområder, skal Leverandøren ikke honoreres for tidsforbrug til uddybende inspektion vedrørende dette, eller til yderligere tidsforbrug mv. til afhjælpning af dette.

10.3 Leverandøren skal én gang årligt vederlagsfrit fremsende en erklæring om overholdelse af denne Aftale. Erklæringen skal udarbejdes i overensstemmelse med gældende, anerkendte branchestandarder på området, og skal omfatte både Leverandørens og eventuelle underdatabehandleres databehandling. Erklæringen udarbejdes som en generel erklæring over Leverandørens databehandling for alle Leverandørens kunder. Første erklæring fremsendes til Kunden senest 12 måneder efter indgåelsen af nærværende aftale.

10.4 I tilfælde af, at relevante offentlige myndigheder, særligt Datatilsynet, foretager en inspektion hos Leverandøren af forhold, der ikke udspringer af Hovedaftalen mellem Leverandøren og Kunden er det uden udgift for Kunden.

10.5 I tilfælde af, at Kunden og/eller relevante offentlige myndigheder, særligt Datatilsynet, foretager en inspektion hos Leverandøren af forhold, der udspringer af Hovedaftalen mellem Leverandøren og Kunden, forpligter Leverandøren og Leverandørens underleverandører sig til overfor Kunden at stille tid og ressourcer til rådighed herfor mod, at Kunden friholder Leverandøren og Leverandørens underleverandører for enhver rimelig udgift i forbindelse med inspektionen. I det omfang, der i forbindelse med inspektionen måtte blive konstateret problematiske forhold vedrørende Leverandørens ansvarsområder, skal Leverandøren ikke honoreres for tidsforbrug til uddybende inspektion vedrørende dette, eller til yderligere tidsforbrug mv. til afhjælpning af dette.

11. Ændringer i Aftalen

11.1 Kunden kan til enhver tid, med et forudgående varsel på mindst 30 dage, foretage ændringer i Aftalen og instruksen, jf. bilag 3. Ændringsprocessen og omkostningerne aftales skriftligt mellem Kunden og Leverandøren i Hovedaftalen. Leverandøren skal ved sådanne ændringer uden ugrundet ophold sikre, at underdatabehandlerne tillige forpligtes af ændringerne.

11.2 I det omfang ændringer i lovgivningen, jf. pkt 1.1 og 1.2, eller tilhørende praksis, giver anledning til dette, er Kunden med et varsel på 30 dage og uden at dette medfører krav om betaling fra Leverandøren, berettiget til at foretage ændringer i Aftalen.

12. Sletning af data

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

12.2 Kunden skal senest 30 dage inden Hovedaftalens ophør skriftligt meddele Leverandøren, hvorvidt alle personoplysningerne skal slettes eller tilbageleveres til Kunden. I det tilfælde, hvor personoplysningerne tilbageleveres til Kunden, skal Leverandøren ligeledes slette eventuelle kopier. Leverandøren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever Kundens meddelelse.

12.3 Leverandøren skal fremsende dokumentation for, at den påkrævede sletning, jf. pkt. 12.2, er foretaget.

13. Misligholdelse og tvistigheder

13.1 Hovedaftalens bestemmelser om misligholdelse og tvistigheder skal også gælde for denne Aftale.

14. Erstatning, ansvarsbegrænsning og forsikring

14.1 Hovedaftalens bestemmelser om erstatning, ansvarsbegrænsning og forsikring skal også gælde for denne Aftale.

14.2 Ud over de almindelige forældelsesregler gælder, at Leverandørens ansvar ophører 5 år efter Hovedaftalens eller 5 år efter delaftales ophør.

15. Ikrafttræden og varighed

15.1 Aftalen indgås ved begge parters underskrift og løber indtil ophør af Hovedaftalen.

16. Formkrav

16.1 Aftalen skal foreligge skriftligt, herunder elektronisk, hos Kunden og Leverandøren.

17. Kontaktpersoner/ Kontaktpunkter hos den dataansvarlige og databehandleren vedrørende databehandleraftalen og ved databrud

17.1 Parterne kan kontakte hinanden via nedenstående kontaktpersoner/kontaktpunkter

17.2 Parterne er forpligtiget til løbende at orientere hinanden om ændringer vedrørende kontaktpersonen/kontaktpunktet

Navn:	Anders Krøjmand Humle	Navn:	
Stilling:	Gruppeleder	Stilling:	
Telefonnr:	4348 6994	Telefonnr:	
Email:	Anderskroj-mand.humle@sweco.dk	Email:	

18. Underskrift

For Kunden
Dato 2018-2018

For Leverandøren
Dato: 15. august 2018

Bilag:
Bilag 1 – Sikkerhed
Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)
Bilag 3 – Instruks

SWECO

Bilag 1 – Sikkerhed

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 2.

2. Sikkerhedskrav indtil 25. maj 2018

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der opfylder kravene i Sikkerhedsbekendtgørelsen og tilhørende praksis.

Foranstaltningerne gennemføres for at undgå, at personoplysninger:

- tilintetgøres, mistes, ændres eller forringes,
- kommer til uvedkommendes kendskab eller misbruges,
- eller i øvrigt behandles i strid med lovgivningen, jf. Aftalens pkt. 1.1

Generelle sikkerhedsforanstaltninger
[Her beskriver Leverandøren, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 2 om interne sikkerhedsbestemmelser, instrukser, retningslinjer for Leverandørens tilsyn og ajourføring, instruktion, fysisk sikring samt sikkerhed ved reparation, service, kassation af medier mv.]

Sweco GIS&IT har implementeret alt login baseret på 2 domæner, til hhv. produktions- og udviklingsmiljøerne. Således er alt login centralstyret. Adgang til de centrale domæne servere og administration af brugere (oprettelse og nedlæggelse) påhviler GIS&IT driftsgruppe. Brugerne kan til enhver tid selv skifte password, så længe det overholder standarden for 8 karakterer, inklusiv små og store bogstaver, tal og special tegn. Brugere deaktiveres og fratages alle rettigheder ved ansættelsesophør. Ved oprettelse af nye brugere (nyansatte) sættes disse ind i forholdene og reglerne for adgangsbrugen til den/de services, der gives adgang til, af GIS&IT driftsgruppe.

Alle servere er virtuelle, og ved endt anvendelse i relation til et projekt, slettes projektdedikerede servere fra produktion og udviklingsmiljøer. Alle ændringer til produktions- og udviklingsmiljøerne, der ikke er applikationsændringer, sker via Swecos issuetrackersystem, der således fungerer som change management platform.

Swecos produktionsmiljø indeholder begrænset omfang af personoplysninger, og disse er afskærmet for uvedkommende via applikationslaget, og der gives kun adgang for relevante projektmedarbejdere til servere og database – udover Swecos GIS&IT driftsgruppe.

GIS&IT hosting operatør Rackhostings personale har adgang til alle servere på administrativt niveau. Underdatabehandleraftale indgået mellem Sweco og Rackhosting, som beskriver Rackhostings sikkerhedsforanstaltninger, kan rekvireres ved behov.

Autorisation og adgangskontrol
[Her beskriver Leverandøren, hvordan Leverandøren overholder kravene i Sikkerheds-bekendtgørelsens kap. 2, samt hvis relevant kap. 3, om autorisationer og adgangskontrol]

Adgang til RenoWeb og Renoweb databasen hos Sweco:
Alle projektdeltagere på RenoWeb projektet har adgang til applikationen via brugergrænsefladen, såfremt de er oprettet som brugere i systemet. Kunden har som systemadministrator adgang til at se, hvilke Sweco brugere der har adgang, og hvilken rolle de er tildelt.

Derudover har udvalgte Sweco Renoweb medarbejdere direkte adgang til databasen. Denne adgang bruges til systemvedligehold og i forbindelse med dataopgaver for Kunden. Dataopgaverne med tilhørende instruks skal bestilles af Kunden. Adgang og databehandling logges på dataopgaveissuet.

Swecos driftsgruppe har administrativ adgang til de servere hvor hhv. database og system er installeret.

Adgang til RenoWeb Office:
Adgangen til RenoWeb Office er konstrueret baseret på unikke brugere og disses kobling til en brugergruppe. Adgangskontroller sker igennem angivelse af brugernavn og gyldig adgangskode. Alle brugere kobles til en rolle, som definerer den enkeltes funktionelle rettigheder.

Adgang til RenoTrack:
Adgang til RenoTrack kontrolcenter sker via adgang til RenoWeb Office, som beskrevet ovenfor.
Adgang til RenoTrack vognklienter (en ios app) sker ved at logge ind på appen med en 6 cifret numerisk kode der identificere Kunden. Derefter hentes brugerinformation fra RenoWeb. Herefter skal brugeren logge ind med sin egen 6 cifrede identifikationskode. Kun brugere der er oprettet i RenoWeb Office som renovatør, kan logge ind i RenoTrack appen. Derudover kræves, at iPad navn er oprettet i RenoWeb Office før systemet giver adgang til data i RenoWeb.

Adgang til RenoMobil:
Adgang til RenoMobil appen (en Android app) sker ved at logge ind på appen med en 6 cifret numerisk kode.
Kun brugere der er oprettet i RenoWeb Office, kan logge ind i RenoMobil appen.

Adgang til Bintag
Adgang til BinTag sker ved at logge ind med en 6 cifret numerisk kode.
Kun brugere der er oprettet i RenoWeb Office, kan logge ind i Bintag

Adgang til Bintag Office
Der er ikke adgangsbeskyttelse på Bintag Office. Denne applikation må derfor kun installeres på computere med adgangskontrol.

Adgang til selvbetjeningsløsninger:
Adgang til selvbetjeningsløsningen kan i dag ske ved brug af NemId/NemLogin eller ved simpel adgang. Det er Kunden som beslutter, hvilken adgangskontrol der skal være på selvbetjeningsløsningen.

Inddatamateriale som indeholder personoplysninger
[Her beskriver Leverandøren, hvis relevant, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 2 om håndtering af inddatamateriale]

Dataopgaver:
Som en del af RenoWeb projektet for Kunden udfører Sweco databehandlingsopgaver, hvor data undersøges og/eller tilrettes til import i RenoWeb. Ofte er der tale om inddatamaterialer i form af eksporteret data fra et af Kundens eksisterende systemer.
Data med personoplysninger må kun leveres over en sikret forbindelse. Hos Sweco placeres disse data midlertidigt på et dataområde, som kun RenoWeb projektmedarbejdere har adgang til. Inddatamaterialet slettes, når dataopgaven er afsluttet og resultatet er godkendt af Kunden.

Inddata til RenoWeb
Renoweb modtager inddata fra følgende kilder og data gemmes direkte i RenoWeb databasen.

- Indtastning via selvbetjeningsløsninger af borgerne og virksomheder
- Indtastning/ opsamling via RenoMobil
- Indtastning via brugerfladen af RenoWeb brugerne
- Indtastning af data via Affaldsportal
- Import fra OIS/ESR
- Import fra CVR
- Import fra dataopgaver
- WMS/WFS fra enten kortforsyning eller Kundens egen GIS afdeling

Uddatamateriale som indeholder personoplysninger
[Her beskriver Leverandøren, hvis relevant, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 2 om håndtering af uddatamateriale]

Renoweb har følgende former for uddatamateriale:

- Rapporter som brugerne kan generere. Her er det brugernes eget ansvar, at uddatamaterialet håndteres i henhold til gældende lovgivning og sikkerhedsbekendtgørelse.
- Videregivelse af telefonnumre og sms tekst til SMS leverandør. Dette sker via en sikret forbindelse til underdatabehandler, som Sweco har/ er ved at indgå underdatabehandleraftale med.
- Videregivelse til andre systemer efter instruks fra kunden. Data videregives via en web-service over en krypteret forbindelse. Det er Kundens ansvar at sikre, at sikkerheden er overholdt hos det modtagende system.
- Selvbetjeningsløsninger som udstilles til borgerne. Her vælger Kunden hvordan adgangen sikres for den enkelte løsning i forbindelse med opsætning af løsningen

- Affaldsportal, hvor borgeren kan se data og få fuld adgang til de selvbetjeningsløsninger, som Kunden har givet adgang til, fra Affaldsportalen.
- Data udstillet igennem standardiserede snitflader (WMS/WFS), som hostes på HTTPS snitflade. Tilgangen til disse services adgangsstyres igennem udlevering af GUID som relateres til Kunden. Adgangen til servicen logges og eventuelle krypterede data dekrypteres i forbindelse med forespørgslen på disse snitflader. Brug af disse services skal håndteres og beskyttes af den dataansvarlige.
- Data udstillet igennem standardiserede snitflader (WMS/WFS), som hostes på HTTPS snitflade med udlevering af et password. Disse snitflader skal inden 25. maj være erstattet af ovenstående snitflademetode med udlevering af en GUID. Kunden vil blive kontaktet såfremt det er relevant for Kundens RenoWeb opsætning.

Eksterne kommunikationsforbindelser
[Her beskriver Leverandøren, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 2 om eksterne kommunikationsforbindelser. Hjælp til udfyldelse kan findes i Datatilsynets it-sikkerhedstekster: https://www.datatilsynet.dk/publikationer/it-sikkerhedstekster/]

Al ekstern tilgang til Swecos hostede applikationer sker via internet, via HTTPS protokollen der er sat op med TLS 1.2 eller højere, og med en ciphersuite der sørger for, at de fleste klienter kan tilgå systemerne, så længe algoritmerne ikke er på fx CSIS liste over kompromitterede algoritmer. Desuden er det standard, at applikationerne HSTS enables med preload option.

Al intern tilgang til Swecos hostede applikationer og servere sker via en punkt-til-punkt MPLS fibernet-forbindelse mellem Sweco og serverfarmen i Rackhostings datacenter – denne forbindelse er således privat og krypteret under transmissionen.

Der udstedes ingen adgang til serverfarmen eksternt, kun Swecos interne personale har adgang, og kun i de nævnte grupper (projektmedarbejdere i begrænset omfang, driftsgruppen og hosting operatøren på administrativt niveau).
I tilfælde af kabelbrud kan GIS&IT driftsgruppe få forbindelse til serverfarmen via en VPN forbindelse, hvorigennem kun driftsgruppens personale har adgang til at forbinde.

Når GIS&ITs offshore personale arbejder på projekter i udviklingsmiljøet sker dette via en VPN forbindelse. Offshore personale har ikke adgang til data, medmindre dette er aftalt specifikt i instruksen.

I særlige tilfælde hvor en kunde kræver eksklusiv adgang til en server, der går udover applikationen, udskilles denne fra serverfarmen og opstilles som "stand-alone-server", og al adgang til serveren sikres med ip låsninger og firewalling for at sikre, at kun den relevante kunde kan tilegne sig adgang til serverressourcen.

Kontrol med afviste adgangsforsøg
[Her beskriver Leverandøren, hvis relevant, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 3 om kontrol med afviste adgangsforsøg]

Systemet er ikke udviklet til at indeholde følsomme personoplysninger, hvorfor Sikkerhedsbekendtgørelsens kapitel 3 ikke er relevant i forhold til §15. I løbet af 2018 vil RenoWeb indeholde kontrol med afviste adgangsforsøg.

Logning
[Her beskriver Leverandøren, hvis relevant, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 3 om logning]

IP-adresser logges via Nagios i hosting miljøet.

RenoWeb er ikke implementeret til at indeholde personfølsomme data, hvorfor logning i henhold til Sikkerhedsbekendtgørelsens kapitel 3 ikke er relevant i henhold til §15.

Inden udgangen af 2018 vil der i RenoWeb være logning af alle behandlinger på fritekstfelter.

Log gemmes i henhold til instruksen fra Kunden – se bilag 3.

Hjemmearbejdspladser
Leverandørens behandling af personoplysninger sker helt eller delvist ved anvendelse af hjemmearbejdspladser [*Leverandøren udfylder*]:
☒ Ja
☐ Nej
[Her beskriver Leverandøren, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 2 om retningslinjer for hjemmearbejdspladser mv.]

I forbindelse med hjemmearbejdspladser gælder følgende regler:

- Medarbejdere der arbejder fra hjemmearbejdsplads/fjernarbejdsplads arbejder på den af firmaet udleverede bærbare arbejdscomputer.
- Kunders data skal opbevares i hosting miljøet og må ikke nedtages lokalt på arbejdscomputeren. Er der situationer, hvor det er nødvendigt at nedtage data fra hostingmiljøet, må dette kun ske til krypterede medier og data skal slettes efter brug.
- Medarbejderen kobler op fra sin bærbare firma computer til Swecos miljø via VPN (Krypteret forbindelse). Fra Swecos miljø kan medarbejderen komme videre til den hostede løsning.
- Der må ikke ske trådløst print af data på hjemmearbejdsplads/fjernarbejdsplads. Såfremt det er nødvendigt at foretage print på hjemmearbejdspladsen gælder, at medarbejderen skal sikre sig, at andre ikke kan få adgang til printet (dvs. det må ikke ske til en printer der gemmer print i hukommelsen og man skal sikre at ingen andre kan tage printet fra printeren).
- Medarbejderen skal sikre sig, at data på print ikke kommer i andres hænder og at print bliver destrueret i forbindelse med udsmidning.

Kommunikationsværktøj - GCBIT Servicedesk
Kundens brugere kan melde om problemer via mail til support eller ved brug af GIS & ITs Collaboration Bug and Issue Tracker Servicedesk portal. Mails sendt til support@renoweb.dk registreres automatisk i GCBIT og brugerens email registreres i systemet.

I portalen kan en bruger kan kun se egne issues, medmindre Kunden har bedt Sweco om at brugerne i Kundens organisation skal kunne se hinandens issues. Kunden er ansvarlig for, at kun brugere der har lov til at se issues omhandlende Kundens projekt er med i organisationen. Derudover er Kunden ansvarlig for at sikre at brugere slettes i Servicedesk, når de ikke længere skal have adgang til Kundens issues.

GCBIT Servicedesk er underlagt de samme generelle sikkerhedsforanstaltninger som beskrevet ovenfor.

3. Sikkerhedskrav fra 25. maj 2018

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, jf. Instruks (bilag 3), og som dermed opfylder Databeskyttelsesforordningens artikel 32.
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 3)
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

Swecos afdelinger GIS&IT, Pavement Consulting og Facility Management har en fælles informationssikkerhedspolitik for softwareudvikling, hosting og drift af IT-systemer som supplerer Swecos generelle informationssikkerhedspolitik. I henhold til denne aftale følges denne informationssikkerhedspolitik for at sikre at sikkerhedsniveauet passer til de aftalte behandlinger.
Informationspolitikken er baseret på ISO27001/02 og består af kontroller indenfor følgende hovedområder:

- A5 Informationssikkerhedspolitikker
- A6 Organisering af informationssikkerhed
- A7 Personale sikkerhed
- A8 Styring af aktiver
- A9 Adgangsstyring
- A10 Kryptografi
- A11 Fysisk sikring og miljøsikring
- A12 Driftssikkerhed
- A13 Kommunikationssikkerhed
- A14 Anskaffelse, udvikling og vedligeholdelse af systemer
- A15 Leverandør forhold
- A16 Styring af informationssikkerhedsbrud

- A17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- A18 Overensstemmelse
- A20 Databehandler aftaler
- A21 Konsulentadgange hos kunder

Målene for informationssikkerhedspolitikken er:

- Høj driftssikkerhed med høj oppetid, minimeret risiko for større nedbrud og datatab
- Fortrolig behandling, transmission og opbevaring af data, hvor kun autoriserede og autentificerede brugere har adgang og hvor brugerens adgang er begrænset til det nødvendige
- Overholdelse af persondataforordningen og generel lovgivning

Informationspolitikken vurderes og revideres minimum en gang årligt sammen med risikovurdering af hosting- og udviklingsmiljøet.
Informationssikkerhedspolitikkens kontroller overvåges af Sweco GIS&ITs driftsgruppe, som har ansvar for at hosting, test og udviklingsmiljøet er kørende og sikkerhedsmæssigt up to date. De enkelte produkter/systemers sikkerhed varetages af produktet/projektet under overholdelse af informationssikkerhedspolitikken.
Herunder er de overordnede sikkerhedsforanstaltninger beskrevet for hosting, test og udviklingsmiljøet efterfulgt af en overordnet beskrivelse af de sikkerhedsforanstaltninger der er indarbejdet i produktet/systemet og organiseringen omkring dette.

Generelle sikkerhedsforanstaltninger:

Fysiske sikkerhedsforhold
Vores hostingoperatør sørger for de fysiske sikkerhedsforhold i form af:

- Alle data flyttes til sekundært DC hvert kvarter
- Datacentre er S40 forsikringsklassificeret
- Elektronisk 2 faktor adgangskontrol.
- Skafor rød sikret bygningsskal
- Dobbelt fremført bystrøm
- Sikret mod oversvømmelse
- Brandsikring
- Fuld kameraovervågning
- Bemandet døgnovervågning
- Dobbelt adgangssluse med alarm mod samtidige åbninger
- Redundante UPS
- Diesel generator
- Simuleret generator test hver 3. måned
- Årlig fuld-last generatortest m. lukning af bystrøm
- 4 x 10 GB fiber backbones
- Altid link på min. 3 backbones
- Forsikring mod brand, vand og tyveri

IT og datasikkerhed

- Al login er centralstyret og baseret på 2 domæner, hhv. produktions- og udviklingsmiljøerne. Adgang til de centrale domæne servere og administration af brugere (oprettelse og nedlæggelse) påhviler GIS&IT driftsgruppe. Brugerne kan til enhver tid selv skifte password, så længe det overholder standarden i informationssikkerhedspolitikken. Brugere deaktiveres og fratages alle rettigheder, ved ansættelsesophør. Ved oprettelse af nye brugere (nyansatte) sættes disse ind i forholdene og reglerne for adgangsbrugen til den/de services, der gives adgang til, af GIS&IT driftsgruppe, før de får adgang.
- Alle servere er virtuelle, og ved endt anvendelse i relation til et projekt, slettes projektdedikerede servere fra produktion og udviklingsmiljøer. Alle ændringer til produktions- og udviklingsmiljøerne, der ikke er applikationsændringer, sker via Swecos issuetrackersystem, der således fungerer som change management platform.
- Swecos produktionsmiljø indeholder i begrænset omfang af personoplysninger, og disse er afskærmet for uvedkommende via applikationslaget, og der gives kun adgang for relevante projektmedarbejdere til servere og database – udover Swecos GIS&IT driftsgruppe.
- GIS&IT hosting operatør Rackhostings personale har adgang til alle servere på administrativt niveau. Underdatabehandleraftale indgået mellem Sweco og Rackhosting, som beskriver Rackhostings sikkerhedsforanstaltninger, er vedlagt.
- Der er implementeret fuld ind- og udgående spam- og virusscanning af mail.
- Der er implementeret central antivirus administration som installeres på alle servere som vores hosting operatør opretter.
- Både vores hostingoperatør og Sweco har implementeret central logning af alle relevante enheder (infrastruktur og servere)
- Vores hostingoperatør sørger for, at der er implementeret Intrusion Detection/Prevention Systemer
- Der benyttes Nagios til drifts- og applikations overvågning og alarmering.
- Al ekstern tilgang til Swecos hostede applikationer sker via internet, via HTTPS protokollen der er sat op med TLS 1.2 eller højere, og med en ciphersuite der sørger for, at de fleste klienter kan tilgå systemerne, så længe algoritmerne ikke er på fx CSIS liste over kompromitterede algoritmer. Desuden er det standard, at applikationerne HSTS enables med preload option.
- Al intern tilgang til Swecos hostede applikationer og servere sker via en punkt-til-punkt MPLS fibernet-forbindelse mellem Sweco og serverfarmen i Rackhostings datacenter – denne forbindelse er således privat og krypteret under transmissionen.
- Der udstedes ingen adgang til serverfarmen eksternt, kun Swecos interne personale har adgang, og kun i de nævnte grupper (projektmedarbejdere i begrænset omfang, driftsgruppen og hosting operatøren på administrativt niveau).
- I tilfælde af kabelbrud kan GIS&IT driftsgruppe få forbindelse til serverfarmen via en VPN forbindelse, hvorigennem kun driftsgruppens personale har adgang til at forbinde.
- Når GIS&ITs offshore personale arbejder på projekter i udviklingsmiljøet sker dette via en VPN forbindelse.
- I særlige tilfælde hvor en kunde kræver eksklusiv adgang til en server, der går udover applikationen, udskilles denne fra serverfarmen og opstilles som "stand-

alone-server", og al adgang til serveren sikres med ip låsninger og firewalling for at sikre, at kun den relevante kunde kan tilegne sig adgang til serverressourcen.

Organisatoriske foranstaltninger

- Alle ansatte har personligt login til Swecos platform
- Alle relevante ansatte har personligt login til hhv hosting- og udviklingsmiljø
- Alle ansatte har rettigheder baseret på behov
- Alle ansatte bærer identifikationskort
- Ansatte er funktionsadskilt i forhold til produktionsdata og backup data
- Ingen ansatte får adgang til personoplysninger, før de er blevet bekendtgjort med den instruks der gælder for behandling af personoplysningerne
- Adgange og autorisation kontrolleres jævnligt

Hjemmearbejdspladser

I forbindelse med brug af hjemmearbejdspladser gælder følgende regler:

- Medarbejdere der arbejder fra hjemmearbejdsplads/fjernarbejdsplads arbejder på den af firmaet udleverede bærbare arbejdscomputer.
- Kunders data skal opbevares i hosting miljøet eller kundens miljø og må ikke nedtages lokalt på arbejdscomputeren. Er der situationer, hvor det er nødvendigt at nedtage data fra hostingmiljøet, må dette kun ske til krypterede medier og data skal slettet efter brug.
- Medarbejderen kobler op fra sin bærbare firma computer til Swecos miljø via VPN (Krypteret forbindelse). Fra Swecos miljø kan medarbejderen komme videre til den hostede løsning.
- Der må ikke ske trådløst print af data på hjemmearbejdsplads/fjernarbejdsplads. Såfremt det er nødvendigt at foretage print på hjemmearbejdspladsen gælder, at medarbejderen skal sikre sig, at andre ikke kan få adgang til printet (dvs. det må ikke ske til en printer der gemmer print i hukommelsen og man skal sikre at ingen andre kan tage printet fra printeren).
- Medarbejderen skal sikre sig, at data på print ikke kommer i andres hænder og at print bliver destrueret i forbindelse med udsmidning.

Kommunikationsværktøj

GCBIT Servicedesk

Kundens brugere kan melde om problemer via mail til support eller ved brug af GIS & ITs Collaboration Bug and Issue Tracker Servicedesk portal. Mails sendt til support@re-noweb.dk registreres automatisk i GCBIT og brugerens email registreres i systemet.

I portalen kan en bruger kan kun se egne issues, medmindre Kunden har bedt Sweco om at brugerne i Kundens organisation skal kunne se hinandens issues. Kunden er ansvarlig for, at kun brugere der har lov til at se issues omhandlende Kundens projekt er med i organisationen. Derudover er Kunden ansvarlig for at sikre at brugere slettes i Service-desk, når de ikke længere skal have adgang til Kundens issues.

GCBIT Servicedesk er underlagt de samme generelle sikkerhedsforanstaltninger som beskrevet ovenfor.

Produkt/system sikkerhedsforanstaltninger:

Autorisation og adgangskontrol
Adgang til RenoWeb og Renoweb databasen hos Sweco:
Alle projektdeltagere på RenoWeb projektet har adgang til applikationen via brugergrænsefladen, såfremt de er oprettet som brugere i systemet. Kunden har som systemadministrator adgang til at se, hvilke Sweco brugere der har adgang, og hvilken rolle de er tildelt.

Derudover har udvalgte Sweco Renoweb medarbejdere direkte adgang til databasen. Denne adgang bruges til systemvedligehold og i forbindelse med dataopgaver for Kunden. Dataopgaverne med tilhørende instruks skal bestilles af Kunden. Adgang og databehandling logges på dataopgaveissuet.

Swecos driftsgruppe har administrativ adgang til de servere hvor hhv. database og system er installeret.

Adgang til RenoWeb Office:
Adgangen til RenoWeb Office er konstrueret baseret på unikke brugere og disses kobling til en brugergruppe. Adgangskontrol sker gennem angivelse af brugernavn og gyldig adgangskode. Adgangskoden defineres efter gældende procedurebeskrivelse i Swecos informationssikkerhedspolitik. Alle brugere kobles til en rolle, som definerer den enkeltes funktionelle rettigheder. Det er i RenoWeb muligt at specialisere brugeradgangen til data og funktionalitet for den enkelte bruger udover rolle begrebet, så adgang kan begrænses yderligere.

Adgang til RenoTrack:
Adgang til RenoTrack kontrolcenter sker via adgang til RenoWeb Office, som beskrevet ovenfor.
Adgang til RenoTrack vognklienter (en ios app) sker ved at logge ind på appen med en 6 cifret numerisk kode der identificere Kunden. Derefter hentes brugerinformation fra RenoWeb. Herefter skal brugeren logge ind med sin egen 6 cifrede identifikationskode. Kun brugere der er oprettet i RenoWeb Office som renovatør, kan logge ind i RenoTrack appen. Derudover kræves, at iPad navn er oprettet i RenoWeb Office før systemet giver adgang til data i RenoWeb. I løbet af 2018 forbedres sikkerheden på RenoTrack ved at adgang til RenoTrack appen (en iOS app) sker ved at logge ind på appen med en adgangskode, som defineres efter gældende procedurebeskrivelse i Swecos informationssikkerhedspolitik. Kun brugere der er oprettet i RenoWeb Office, kan logge ind i RenoTrack appen.
Indtil da, anbefaler Sweco at RenoMobil kun benyttes på krypterede enheder. Såfremt IPAD kører IOS 8 eller højere vil IPAD pr default være krypteret.

Adgang til RenoMobil:
Adgang til RenoMobil appen (en Android app) sker ved at logge ind på appen med en 6 cifret numerisk kode.
I løbet af 2018 forbedres sikkerheden på RenoMobil ved at adgang til RenoMobil appen (en Android app) sker ved at logge ind på appen med en adgangskode, som defineres efter gældende procedurebeskrivelse i Swecos informationssikkerhedspolitik. Kun brugere der er oprettet i RenoWeb office, kan logge ind i RenoMobil appen.

En øget sikkerhed kan også opnås, såfremt enheden hvorpå RenoMobil benyttes er krypteret.

Adgang til Bintag
Adgang til BinTag app sker ved at logge ind med en 6 cifret numerisk kode.
Kun brugere der er oprettet i RenoWeb Office, kan logge ind i Bintag
I løbet af 2018 forbedres adgangssikkerheden på bintag app.

Adgang til Bintag Office
Der er ikke adgangsbeskyttelse på Bintag Office. Denne applikation må derfor kun installeres på computere med adgangskontrol.
I løbet af 2018 forbedres adgangssikkerheden til Bintag office.

Adgang til selvbetjeningsløsninger:
Adgang til selvbetjeningsløsningen kan i dag ske ved brug af NemId/NemLogin eller simpel adgang. Det er Kunden som beslutter, hvilken adgangskontrol der skal være på selvbetjeningsløsningen.

RenoWeb Office indeholder logning af afviste adgangsforsøg og mulighed for at opsætte spærring ved for mange forgæves loginforsøg.

Inddatamateriel som indeholder personoplysninger
Renoweb modtager inddatamateriel fra følgende kilder og gemmes direkte i RenoWeb databasen og er beskyttes via produktets generelle beskyttelse.

- Indtastning via selvbetjeningsløsninger af borgerne og virksomheder
- Indtastning/ opsamling via RenoMobil
- Indtastning via brugerfladen af RenoWeb brugerne
- Indtastning af data via Affaldsportal
- Import fra OIS/ESR
- Import fra CVR
- Import fra dataopgaver
- WMS/WFS fra enten kortforsyning eller Kundens egen GIS afdeling

Dataopgaver:
Som en del af RenoWeb projektet for Kunden udfører Sweco databehandlingsopgaver, hvor data undersøges og/eller tilrettes til import i RenoWeb. Ofte er der tale om inddatamaterialer i form af eksporteret data fra et af Kundens eksisterende systemer.
Data med personoplysninger må kun leveres over en sikret forbindelse. Hos Sweco placeres disse data midlertidigt på et dataområde, som kun RenoWeb projektmedarbejdere har adgang til. Inddatamaterialet slettes, når dataopgaven er afsluttet og resultatet er godkendt af Kunden.

Uddatamateriale som indeholder personoplysninger
Renoweb har følgende former for uddatamateriale:

- Rapporter som brugerne kan generere. Her er det brugernes eget ansvar, at uddatamaterialet håndteres i henhold til gældende lovgivning og sikkerhedsbekendtgørelse
- Videregivelse af telefonnumre og sms tekst til SMS leverandør. Dette sker via en sikret forbindelse til underdatabehandler.
- Videregivelse til andre systemer via webservice efter instruks fra kunden. Data videregives via en webservice over en krypteret forbindelse. Det er Kundens ansvar at sikre, at sikkerheden er overholdt hos det modtagne system.
- Videregivelse til andre systemer via fil efter instruks fra kunden. Nogle RenoWeb koblinger er via filoverførsel. Her danner RenoWeb filen, men det er Kundens ansvar at filen overføres til det modtagne system.
- Selvbetjeningsløsninger som udstilles til borgerne. Her vælger Kunden hvordan adgangen sikres for den enkelte løsning i forbindelse med opsætning af løsningen
- Affaldsportal, hvor borgeren kan se data og få fuld adgang til de selvbetjeningsløsninger, som Kunden har givet adgang til, fra Affaldsportalen.
- Data udstillet igennem standardiserede snitflader (WMS/WFS), som hostes på HTTPS snitflade. Tilgangen til disse services adgangsstyres igennem udlevering af GUID som relateres til Kunden. Adgangen til servicen logges og eventuelle krypterede data dekrypteres i forbindelse med forespørgslen på disse snitflader. Brug af disse services skal håndteres og beskyttes af den dataansvarlige.

Logning
IP-adresser logges via Nagios i hosting miljøet.

RenoWeb logger afviste adgangsforsøg og der spærres for adgang til RenoWeb i en parameterstyret periode, hvis der har været mere end et antal (parameterstyret) forsøg.

I RenoWeb logges hvis brugere forsøger at tilgå data/funktionalitet, som deres rolle ikke har adgang til.

I løbet af 2018 udvides RenoWeb til at logge al behandling af fritekst felter, da disse felter, selv om de ikke er beregnet til følsomme personoplysninger, ikke kan sikres mod at brugere skriver personfølsomme oplysninger i felterne.

Log gemmes i henhold til instruksen fra Kunden – se bilag 3.

Data

Dataopbevaringssted	Data opbevares	Type
Kundes eget miljø	Nej	
Hosting milljø	Ja	Database
Hosted udviklingsmiljø	Ja	Databaser i forbindelse med test og databehandlingsopgaver

Dataopbevaringssted	Data opbevares	Type
Swecos miljø	Ja	Databaser og modtagne inddata i forbindelse med databehandlingsopgaver
Arbejdspc'er	I få tilfælde	Kun i sjældne tilfælde i forbindelse med databehandlingsopgaver. I disse tilfælde vil det kun være på en krypteret arbejdspc.

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)

1. **Lokation(er) for behandlingen** *[Her opregner Leverandøren, de steder, hvor Kundens personoplysninger opbevares/behandles.]*

   Hosting - Rackhosting, Hørskætten 6c, 2630 Taastrup og Hørskætten 3-5, 2630 Taastrup

   Driftsovervågning og support – Sweco Danmark. Swecos kontoradresser i Danmark fremgår af Sweco.dk.

   Brug af RenoWeb office - Internettet (Kunden, renovatør, og evt. andre brugere som kunden giver adgang)
   Brug af selvbetjeningsløsninger - Internettet (borgere, Kunden, virksomheder)
   Brug af RenoMobil (Renovatør)
   Brug af RenoTrack (Renovatør, Kunden)

   SMS meddelelser
   LINK Mobility A/S
   Copenhagen Towers Ørestads Boulevard 114-118
   2300 København S, Denmark
   +4570261272
   www.linkmobility.com

   Underdatabehandler aftale kan rekvireres ved behov.

   Data vedrørende sms beskeder og telefonnumre opbevares på Link Mobilitys datacenter på adressen:

   Storsätragränd 3
   127 39 Skärholmen
   Sverige

   Data vedrørende PDF-kalender opbevares på Kortermann-ITs datacenter på adressen:

   Englandsvej 8
   5700 Svendborg

   Opbevaring af data i forbindelse med dataopgaver – se afsnit Lokation(er) for opbevaring af data ud over behandlingssteder.

2. **Lokation(er) for opbevaring af data ud over behandlingssteder**

   Data som bearbejdes i forbindelse med projektet uden for hosting miljøet, f.eks. i forbindelse med klargøring til hosting eller analyser af data opbevares på Swecos servere som befinder sig på følgende lokationer:

   Sentia
   Smedeland 32
   2600 Glostrup

Backup findes lokalt på ovenstående adresse samt som en sekundær backup hos
Sungard Availability Services, DC Sollentuna, Bäckvägen 18,
192 54 Sollentuna

Data som leveres til Sweco via Sweco Secure File Transfer opbevares midlertidigt i følgende datacenter
DC Sollentuna
Bäckvägen 18
192 54 Sollentuna

Og redundant miljø
DC Sätra
Stensätravägen 13
127 39 Skärholmen

For ovenstående leverandører af datacenter gælder, at de ikke har adgang til de servere, hvorpå data befinder sig, hvorfor der ikke er indgået databehandleraftaler med disse.

3. **Underdatabehandlere** *[Her angiver Leverandøren navn, adresse, cvr-nummer m.m. på underdatabehandlere, som er godkendt af Kunden, jf. pkt. 5.2 i Aftalen.]*

Systemet hostes hos Rackhosting, Hørskætten 6c, 2630 Taastrup, CVR: 15777176.
Underdatabehandler aftale kan rekvireres ved behov.

Fra systemet sendes SMS ved brug af
Link Mobility A/S, Birkemose Allé 37 6000 Kolding, CVR: 30077250
Underdatabehandleraftale kan rekvireres efter 1. april 2018.

PDF-kalender
Kortermann-IT Englandsvej 8, 5700 Svendborg, CVR: 29794200
Underdatabehandleraftale kan rekvireres efter 1. april 2018.

Der er ikke indgået databehandleraftaler med de leverandører, der stiller fysisk plads til rådighed for Swecos servere, da de ikke har adgang til serverne og derved data.

Bilag 3 – Instruks

Instruks
Kunden instruerer hermed Leverandøren om at foretage behandling af Kundens oplysninger til brug for hosting og support af RenoWeb, jf. Hovedaftalen.

Leverandøren er ansvarlig for, at Kundens instruks fremsendes til eventuelle underdatabehandlere.

1.1 Behandlingens formål

Behandling af Kundens oplysninger sker i henhold til formålet i Hovedaftalen og er uddybet i den generelle beskrivelse af behandlingen i dette bilag

Leverandøren må ikke anvende oplysningerne til andre formål.
Oplysningerne må ikke behandles efter instruks fra andre end Kunden.

Kunden og Leverandøren kan aftale at udvide eller indskrænke instruksen i bilag 3. Aftale om ændring af instruks vedlægges som et tillæg til instruksen, jf. dette bilag.

1.2 Generel beskrivelse af behandlingen

[Her beskriver Kunden udførligt de typer af behandling, som Leverandøren skal udføre, herunder processer, varigheden og karakteren af behandlingen.]

Leverandøren er ansvarlig for support, vedligehold, videreudvikling og hosting af RenoWeb.
Leverandørens behandling af data består af:

- Hosting af data.
- Sikring af data.
- Backup af data.
- Brug af data i anonymiseret form til test og udvikling af RenoWeb
- Kig på data i forbindelse med besvarelser på supporthenvendelser. Herunder test af fejl, som skyldes problemer med data.
- Bearbejdning af data i forbindelse med konkrete databehandlingsopgaver. Den specifikke instruks til behandlingen af data i forbindelse med dataopgaver gives af Kunden i forbindelse med bestilling af dataopgaven og dokumenteres i opgavebeskrivelsen.
- Opsamling af statistik på de mobile RenoWeb moduler til forbedring af løsningen.
- Videregivelse af data gennem opsatte koblinger.
- Videregivelse af data via opsatte WMS/WFS services.

Systemet er sat op med følgende koblinger:

SMS-kobling
RenoWeb sender telefonnumre og sms-tekst til Link Mobility A/S (underdatabehandler), som sørger for at sende SMS til de tilmeldte borgere.

PDF-kalender
RenoWeb sender adresse og tømmedatoer til Kortermann-IT (underdatabehandler).

Koblinger til eksterne systemer:
For alle nedenstående eksterne koblinger gælder, at det er Kundens ansvar som dataansvarlig at sikre, at der er lovhjemmel til at hente data til/ overføre data fra RenoWeb, at data behandles forsvarligt i det eksterne system, og at den overførselsmetode, som det eksterne system stiller til rådighed, har den nødvendige sikkerhed.

Import fra OIS/ESR
RenoWeb importerer oplysninger om adresser, ejendomme, ejeroplysninger og ejer administrator oplysninger i Kundens geografiske område fra OIS/ESR.

Import fra CVR
RenoWeb importerer oplysninger om CVR-nr, p-numre, navne mm i Kundens geografiske område fra CVR.

RenoWeb henter kortlag fra Kortforsyningen (Via Kundens login) eller fra Kundens egen GIS afdeling.

Sweco kan udstille WMS/WFS service på data i RenoWeb, hvis det bestilles af Kunden. Instruks til en sådan service skal gives i forbindelse med opgaven.

Leverandøren hverken registrerer eller anvender data i eller udenfor systemet/systemets koblinger, medmindre der indgås særskilt aftale med Kunden om brug af data til andre formål. Selve databehandlingen foretages af Kunden selv, samt de aktører som Kunden giver adgang til systemet. Det er Kunden, der har ansvaret for, at brugerne af systemet tildeles de korrekte roller og derved rettigheder i forhold til behandlingen af data. Ligeledes er det Kundens ansvar, at der er indgået de nødvendige databehandleraftaler med de leverandører, som systemet efter aftale med Kunden videregiver data til.

RenoWeb udvides i løbet af 2018 med en administrationsside, som gør det muligt for Kunden at slette oplysninger, når der ikke længere er hjemmel til at opbevare oplysningerne i systemet. Indtil denne administrationsside er klar, kan den datasvarlige bestille sletning af data via en dataopgave hos RenoWeb support. Kunden kan derudover under hovedaftalen og mod betaling bede om at få data anonymiseret eller aggregeret inden sletning.

Log om afviste adgangsforsøg og forsøg på brug af funktionalitet som ikke er dækket af brugerens rolle opbevares i 6 måneder.

Leverandøren har lov til at træffe beslutninger om hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe den nødvendige sikkerhed omkring den dataansvarliges oplysninger i systemet, uden at modtage en specifik instruks fra den dataansvarlige.

1.3 Typen af personoplysninger

Behandlingerne indeholder personoplysninger i de nedenfor afkrydsede kategorier. Leverandørens og eventuelle underdatabehandleres niveau for behandlingssikkerhed bør afspejle oplysningernes følsomhed, jf. bilag 1.

Almindelige personoplysninger (indtil 25. maj 2018, jf. Persondatalovens § 6, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 6)
☒ Almindelige personoplysninger

Følsomme personoplysninger (indtil 25. maj 2018, jf. Persondatalovens § 7, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 9):
☐ Racemæssig eller etnisk baggrund
☐ Politisk overbevisning
☐ Religiøs overbevisning
☐ Filosofisk overbevisning
☐ Fagforeningsmæssige tilhørsforhold
☐ Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.
☐ Seksuelle forhold

Oplysninger om enkeltpersoners rent private forhold (indtil 25. maj 2018, jf. Persondatalovens § 8, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 6 og 9):
☐ Strafbare forhold
☐ Væsentlige sociale problemer
☐ Andre rent private forhold, som ikke er nævnt ovenfor:

_____

_____

Oplysninger om cpr-nummer (indtil 25. maj 2018, jf. Persondatalovens § 11, fra 25. maj 2018, eventuelt national lovgivning, jf. Databeskyttelsesforordningens artikel 87)
☐ CPR-numre

RenoWeb er ikke udviklet til at indeholde følsomme personoplysninger, men da RenoWeb indeholder fritekst-felter, hvor der ikke er kontrol på, hvad der skrives, kan det ikke garanteres, at der ikke befinder sig personfølsomme data i RenoWeb.

Sweco har derfor valgt at sikre fritekstfelterne med ekstra logning i RenoWeb fra version ultimo maj 2018.

1.4 Kategorier af registrerede

Der behandles oplysninger om følgende kategorier af registrerede:

Borgere, viceværter, renovatørmedarbejdere der bruger systemet, kundens brugere af systemet.

1.5 Tredjelande (ikke EU-medlemslande)

Leverandøren må overføre personoplysninger til følgende tredjelande:

Ingen.

Versionshistorik

Versionsnr.	Dato	Beskrivelse
12.0	18-04-2018	Udtrædelsesmulighed i 5.2 Præcisering af 6.3 Præsisering af Revisorerklæringsstandard i 10.3 Tilføjelse til 10.2, 10.4 og 10.6 Uddybning af 15.1 Bilag 1. sidst i generelle sikkerhedsforanstaltninger er sætningen 'er vedlagt' erstattet af 'kan rekvireres ved behov' Bilag 1 – sætning med sort fiber fjernet 2 steder. Præciseret, at offshore personale kun har adgang til data, hvis det er aftalt i instruksen Præciseret at GIS&IT, Pavement og Facility Management er afdelinger i Sweco. Bilag 3. Afsnit om 3. lande tilføjet
11.0	21.02.2018	Reformulering af krav 10.6 fra KL's skabelon Bilag 2 udvidet med link til alle Swecos adresser i dk. Tydeligere markering af overskrifter i bilag 1.
10.0	24.01.2018	14.2 forældelsesregel tilføjet.
9.0	23.01.2018	Bilag1 udvidet med beskrivelse gældende efter 25. maj 2018. Formulering i 13.1, 14.1 og 15.1 er rettet, så de sprogligt er ens.
8.0	10.01.2018	Bilag 2 udvidet med fysisk placering af data hos Sweco
7.0	07.12.2017	Krav 10.6 fra KI's skabelon tilføjet – dog tilrettet, så vi ikke gør det gratis. (Hedder 10.4/10.5 i vores)

6.0	27.11.2017	Tilføjelse af at Sweco som databehandler godt må træffe selvstændige beslutninger vedr. tekniske og organisatoriske sikkerhedsforanstaltninger uden at modtage en specifik instruks fra dataansvarlig.
5.0	06.11.2017	Uddybning af krav ved hjemmearbejdsplads
4.0	13.10.2017	Sungard tilføjet som underdatabehandler – de har backup af alle data som vi gemmer på Swecos drev.
3.0	04.10.2017	Tilrettet efter snak med jurist og møde med ledelsen
2.0	11.09.2017	Tilrettet efter kommentarer til JordWeb databehandleraftalen fra flere kunder
1.4	09.08.2017	Tilrettet så det fremgår hvor andre produkter/projekter skal rette for at den kan benyttes.
1.3	30.06.2017	Kommentarer indarbejdet
1.2	08.06.2017	Aftale tilpasset JordWeb og Bygningsaffald.dk
1.1	23.05.2017	Første udkast til aftale for JordWeb og Bygningsaffald.dk
1.0	03.04.2017	Tilrettet efter bemærkninger fra høringsrunde.
0.8	25.11.2016	Høringsudkast på www.kombit.dk