AVTALE

Kunde:	Kragerø kommune			**Org.no.:**	963 946 902
Postadresse:	Pb. 128, 3791 Kragerø		**Besøksadresse:**		Rådhusgata 5, 3770 Kragerø
Kontaktperson:	Adam Eskdale Moen	**Telefon:**	99205726	**E-post:**	adam.moen@kragero.kommune.no

Leverandør:	**Skytech Control AS** (Heretter kalt Leverandør)			**Org.no.:**	922 607 923
Postadresse:	Postboks 2085 Vika, 0125 Oslo		**Besøksadresse:**		Stortingsgata 4, 0161 Oslo
Kontaktperson:	Thomas B. Aaserud	**Telefon:**	**92 08 44 44**	**E-post**	kundeservice@skytechcontrol.io

Estimert antall brukere	**270**	**Avtalt løpetid på avtalen:**	Inntil eventuell oppsigelse

(NB! Evt. datterselskaper som skal inngå i avtalen må eies av moderselskapet med mer enn 50 %, jfr. Aksjeloven av 13. juni 1997 nr. 44, § 1-3.) Slike datterselskap beskrives i så fall i eget vedlegg.

Nåværende teleoperatør:	Telenor - med forbehold om integrasjon
Nåværende leverandør:	Atea/Advania/Dustin - med forbehold om integrasjon
Merknad vedr. teleoperatør:	Avtalen gjelder alle nåværende og fremtidige operatører/leverandører

Priser og betingelser:

TJENESTE	VALGTE TJENESTER	OPPSTART	ETABLERING PR LAND	PRIS
Control plattform totalt			**NOK 20.000,-**	**NOK 29,- pr abo**
Control plattform standard	X	01.01.2025	Inkludert	NOK 0,- pr abo
On- og Offboarding ansatte Abonnement	X	01.01.2025	Inkludert	NOK 0,- pr abo
Fakturahåndtering Avdelingsregnskap og kostnadssplitt privat og jobb	X	01.01.2025	Inkludert	NOK 0,- pr abo
Abonnementshåndtering Kjøp og endringer	X	01.01.2025	Inkludert	NOK 0,- pr abo
Web-shop med egenandel	X	01.01.2025	Min. NOK 0, -	NOK 0,- pr abo
Asset Management Håndtering av utstyr	X	01.01.2025	Min. NOK 0, -	NOK 0,- pr abo
Tilleggstjenester		01.01.2025		
Tap- og skademeldinger Håndtering av utstyr	X	01.01.2025	NOK 0, -	NOK 0, - pr abo
GreenPool Gjenbruk av utstyr	X	01.01.2025	NOK 0, -	NOK 0, - pr abo
SMS SMS Platform for utsendelser			NOK 2.000, -	NOK 0,79 pr SMS
Fil-tilpasning av lønnstrekk fil Tilpasning til ønsket format	X	01.01.2025	Timepris NOK 1.500, -	Ved endringer utover etablering
Fil-tilpasning av regnskaps fil Tilpasning til ønsket format	X	01.01.2025	Timepris NOK 1.500, -	Ved endringer utover etablering
Automatisert HR-dataflyt				Etter avtale

The agreement has been signed digitally by both Parties.

Kragerø Kommune	Skytech Control AS	Skytech Control AS
Adam Moen Adam Moen (Dec 17, 2024 08:05 GMT+1)	Tore Krogstad	Thomas Aaserud Thomas Aaserud (Dec 16, 2024 15:06 GMT+1)
Adam Eskdale Moen IT-sjef	Tore Krogstad CEO	Thomas B. Aaserud Leder Direktesalg

Generelle leveringsvilkår

1. Definisjoner

Avtalen: Signert samarbeidsavtale mellom Kunde og Leverandør samt signert fullmakt
Bruker: En ansatt eller en funksjon som er registrert som ett kostelement med abonnementsnummer på Control plattformen
Produkt: Tilgang til CONTROL plattformen
Oppstart: Tidspunktet da tjenesten er startet og leverandør kan sende første faktura til Kunde. Tidspunkt da tjenesten er startet trer uansett i kraft senest 2 måneder etter signering av kontrakt, dersom oppstart er utsatt på grunn av manglende informasjon fra kunde. Etableringsavgift faktureres umiddelbart etter kontraktsignering.
Part: Leverandør og Kunde, hver for seg benevnt som Part, og i fellesskap som **Partene**
Skriftlig: Partene anser E-post som gyldig skriftlig kommunikasjon
Tjenester: Den leveransen som Avtalen omhandler i henhold til spesifikasjonene på første side

2. Leveransens omfang/kvalitet
Kunde kjøper med dette de Tjenester som er i samsvar med de spesifikasjoner og beskrivelser som følger Avtalen. Dersom Kunde ønsker ytterligere Tjenester, må dette avtales særskilt mellom Partene.

3. Antall Brukere
Antall Brukere av Tjenestene beskrevet i Avtalen vil til enhver tid være det antall kostnadselementer som skaper oppfølgingsbehov fra Leverandør.

4. Kundens ansvar for innhold og bruk
Kunde er ansvarlig for å påse at ingen av Tjenestene fra Leverandør brukes til å formidle ulovlig innhold eller utøve ulovlig handlinger i strid med lovverk eller bransjeetiske regler.

5. Betalingsbetingelser
Forfallstid for betaling av faktura er 30 (tredve) dager. Ved forsinket betaling påløper renter i samsvar med den til enhver tids gjeldende prosentsats etter lov om renter ved forsinket betaling. Pris for leverte Tjenester vil justeres årlig basert på endring i konsumprisindeksen foregående 12 (tolv) måneder.

6. Behandling av personopplysninger
I det omfang Tjenestene innebærer at Leverandør behandler personopplysninger på vegne av Kunde er Leverandør å anse som databehandler. Slik behandling skal skje i henhold til Kundes instruks og reguleres av egen databehandleravtale som vedlegg til denne Avtalen. *Kunde er innforstått med at Leverandør også lagrer, oppbevarer og behandler personopplysninger for levering av tjenestene til kunden, og deres ansatte. Dette som ledd i kundeadministrasjon, regnskapsbehandling, annen nødvendig dokumentasjon samt fakturering forbundet med levering av Tjenestene*. Kunde kan kontakte Leverandør dersom Kunde ønsker mer informasjon om Leverandørs behandling av personopplysninger for egne formål i rollen som behandlingsansvarlig, herunder om Leverandørs grunnlag for slik behandling.

7. Konfidensialitet
Informasjon som en Part eller personer på en Parts side blir kjent med i forbindelse med gjennom- føringen av Avtalen skal behandles konfidensielt og ikke gjøres tilgjengelig for utenforstående uten skriftlig samtykke fra den annen Part.

Dersom ikke annet er avtalt, kan Leverandør benytte Kunde som referansekunde i samsvar med god skikk.

8. Mislighold og misligholdsbeføyelser
8.1. Som mislighold regnes Partenes brudd på plikter etter Avtalen.

8.2.
Ved mislighold har Partene plikt og rett til å foreta utbedring så snart misligholdet er kjent. Dersom en Part ikke lykkes med nødvendig utbedringen innen rimelig tid, kan den annen Part kreve forholdsmessig dekning av egne, dokumenterte kostnader pådratt som en direkte følge av misligholdet. Dersom en Part ikke foretar tilfredsstillende utbedring og dekker den annen Parts dokumenterte kostnader pådratt som en direkte følge av misligholdet og mangelen utgjør et vesentlig kontraktsbrudd, har den annen Part rett til å heve Avtalen på betingelsene angitt i 8.4

8.3. Hver Part kan kreve vederlag for påførte, dokumenterte merutgifter som direkte følge av mislighold fra den annen Parts side.

8.4.
Ved en Parts vesentlig mislighold av Avtalen, kan den annen Part heve Avtalen med 10 (ti) dagers skriftlig varsel.

9. Erstatning
Ved mislighold kan Partene kreve erstatning etter alminnelige erstatningsregler, for dokumentert økonomisk tap. Ingen av Partene er ansvarlig for indirekte tap, herunder tap av data, tap av fortjeneste av enhver art, tap grunnet driftsavbrudd og krav fra tredjepart som følge av en Parts mislighold. Påløpt refusjon og eventuell annen kompensasjon, kommer til fradrag ved erstatningsutmålingen. Leverandørens ansvar er oppad begrenset til et beløpet tilsvarende det Kunden har betalt Leverandøren siste 12 måneder. Ansvarsbegrensningene gjelder likevel ikke ved grov uaktsomhet eller forsett. Leverandør er ikke ansvarlig for tap som følge av uvedkommende sin bruk av Kundes Tjenester, data eller systemer så lenge ikke dette skyldes forhold på Leverandør sin side.

10. Avtalens varighet
10.1. Varighet
Avtalen gjelder f.o.m. begge Parter har signert Avtalen og til oppsigelsestidens utløp, i henhold til pkt. 10.2.

10.2. Oppsigelse
Avtalen har 1 (ett) års bindingstid, regnet fra oppstart av Avtalen, og løper deretter med 3 (tre) måneders gjensidig oppsigelse. En oppsigelse starter å løpe fra den 1. i den påfølgende måned. Oppsigelsen må gjøres Skriftlig mellom partene, til avtalte kontaktpersoner.

11. Overdragelse
Kunde hefter ovenfor Leverandør inntil Leverandør har samtykket til overdragelsen av Avtalen og inntil alle eventuelle utestående fakturaer er innbetalt.

12. Force Majeure
Dersom Avtalens gjennomføring helt eller delvis hindres, eller i vesentlig grad vanskeliggjøres, av forhold som ligger utenfor en Parts kontroll, suspenderes Partenes plikter i den utstrekning aktuelle forhold er relevant, og for så lang tid som forholdet varer. Slike forhold inkluderer, men er ikke begrenset til, streik, lockout, og ethvert forhold som etter norsk rett vil bli vurdert som force majeure. Hver Part kan si opp Avtalen med 1 (én) måneds varsel dersom force majeure- tilfellet gjør det særlig byrdefullt for en Part å opprettholde Avtalen eller dersom situasjonen må antas å vare lenger enn 90 (nitti) dager. Den Part som vil vise til at et slikt forhold hindrer oppfyllelse av Avtalen, skal straks varsle den annen Part Skriftlig om dette.

13. Reklamasjon
Kunde må omgående og senest innen 14 (fjorten) dager etter at mangelen/forsinkelsen/annet mislighold oppdages gi Skriftlig melding til Leverandør.

14. Tvister
Uenighet om virkning, innhold eller gjennomføring av Avtalen skal forsøkes løst ved forhandlinger. Fører ikke forhandlingene frem, kan hver av Partene kreve saken avgjort ved de alminnelige domstoler. Oslo tingsrett er verneting i første instans.

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services ("**Principal Agreement**")

between
Kragerø kommune
(Org.no: 963 946 902)
(the "**Data Controller**")

and
Skytech Control AS
(Org.no: 922 607 923)
(the "**Data Processor**")

(together as the "**Parties**")

WHEREAS

(A) The Data Controller wishes to subcontract certain Services, which imply the processing of Personal Data, to the Data Processor.

(B) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(C) The Parties wish to lay down their rights and obligations.

Version history			
Date	Version	Description	Name
18.12.22	1.0	New template established	Karl Otto Aam (CTO)
03.05.23	1.1	Revised	Karl Otto Aam (CTO)
06.06.23	1.2	Amended clause 5 and 11	Karl Otto Aam (CTO)
21.03.24	1.4	Amended Appendix 1. Section 8	Karl Otto Aam (CTO)
22.05.24	1.5	Amended clause 11.1 and Appendix 1. Section 4. Amended definition under clause 1.1.2	Karl Otto Aam (CTO)

Confidential. All rights reserved to Skytech Control

24.10.24	1.6	Amended Appendix 1. Section 5	Karl Otto Aam (CTO)

Confidential. All rights reserved to Skytech Control

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "**Agreement**" means this Data Processing Agreement and all schedules;

1.1.2 "**Principal Agreement**" means the contract that outlines the overall terms and conditions between the parties involved.

1.1.3 "**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of the Data Controller pursuant to or in connection with the Principal Agreement;

1.1.4 "**Contracted Processor**" means Data Processor and/or a Data Sub-processor;

1.1.5 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.6 "**EEA**" means the European Economic Area;

1.1.7 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.8 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.9 "**Data Transfer**" means:

1.1.9.1 a transfer of Company Personal Data from the Data Controller to a Contracted Processor; or

1.1.9.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.10 "**Services**" means the cost-, user- and asset management services the Data Controller provides.

1.1.11 "**Data Sub-processor**" means any person appointed by or on behalf of Data Processor to process Personal Data on behalf of the Data Controller in connection with the Agreement.

1.2 The terms, "**Commission**", "**Data Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Data Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Data Controller's documented instructions.

2.2 The Data Controller instructs Data Processor to process Company Personal Data. The types of Company Personal Data and the categories of data subjects involved are specified in Appendix 1.

3. Data Processor Personnel

3.1 Data Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know /

Confidential. All rights reserved to Skytech Control

access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Data Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. A detailed description of the Data Processor's information security measures shall be set out in Appendix 2.

4.2 In assessing the appropriate level of security, Data Processor shall take account of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing

5.1 Any use of Data Sub-processors by the Data Processor shall be subject to express prior written information by the Data Controller. Any other legal entity which conducts Processing of Personal Data on behalf of the Data Processor pursuant to this Data Processing Agreement shall be construed as a subcontractor. This applies regardless of whether the subcontractor is partly or fully owned by the Data Processor, by the same parent company as the Data Processor, or is organized within the same company group as Data Processor.

5.2 The Data Controller accepts the Data Processor's use of Data Sub-processors as specified in Appendix 1.

5.3 The Data Processor shall, by written agreement with its subcontractors, ensure that any Processing of Personal Data carried out by a subcontractor is subjected to the same obligations and limitations as those imposed on the Data Processor pursuant to this Data Processing Agreement. The Data Processor shall remain fully liable for Processing of any Controller Personal Data by any of its subcontractors, regardless of whether the Processing was authorized by the Data Processor or the Data Controller.

5.4 If the Data Processor plans to change an existing or add a new subcontractor, it shall notify the Data Controller in writing and obtain the Data Controller's written consent prior to any Processing by the new subcontractor. For the avoidance of doubt, such consent shall not be unreasonably withheld by the Data Controller.

5.5 Should the Data Controller object and withhold its consent in accordance with this section 5, the Parties shall meet and in good faith try to find a solution to mitigate the concerns of the Data Controller. If the Parties cannot agree on a solution, then the Data Controller and the Data Processor shall be entitled to terminate the Data Processing Agreement and the Principal Agreement with three months prior written notice.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Data Processor shall assist the Data Controller by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Data Controller obligations, as reasonably understood by Data Controller, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Data Processor shall:

Confidential. All rights reserved to Skytech Control

6.2.1 promptly notify Data Controller if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Data Controller or as required by Applicable Laws to which the Data Processor is subject, in which case Data Processor shall to the extent permitted by Applicable Laws inform Data Controller of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Data Processor shall notify Data Controller without undue delay upon Data Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Data Controller with sufficient information to allow the Data Controller to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Data Processor shall co-operate with the Data Controller and take reasonable commercial steps as are directed by Data Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Data Processor shall provide reasonable assistance to the Data Controller with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Data Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Company Personal Data

9.1 Subject to this section 9 Data Processor shall promptly and in any event within 30 calendar days of the date of cessation of any Services involving the Processing of Company Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Company Personal Data.

9.2 Data Processor shall provide written certification to Data Controller that it has fully complied with this section 9 within 30 calendar days of the Cessation Date.

10. Audit rights

10.1 Subject to this section 10, Data Processor shall make available to the Data Controller on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Data Controller or an auditor mandated by the Data Controller in relation to the Processing of the Company Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Data Controller only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Data Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for

Confidential. All rights reserved to Skytech Control

the transfer of personal data. The applicable lawful basis for the transfer of Company Personal Data to a third country shall be specified and documented in Appendix 3 of this Data Processing Agreement for each respective Data Sub-processor.

11.2 The Data Processor shall not transfer Data Controller Personal Data to a country outside the European Economic Area ("EEA") or the UK which is not considered to provide an adequate level of protection according to Applicable Data Protection Law ("Third Country"), without the Data Controller's prior written consent. For the avoidance of doubt, this applies also to transfer by way of remote access to Data Controller Personal Data, e.g. customer and technical support. The Data Controller has consented to transfers of Data Controller Personal Data to Third Countries as listed in Appendix 1.

11.3 In any such cases, where the Data Controller has consented to the transfer of Data Controller Personal Data to a Third Country, the Data Processor undertakes to ensure that Data Controller Personal Data is not transferred before adequate safeguards are implemented. This includes but is not limited to ensuring that the EU Standard Contractual Clauses for the Transfer of Personal Data to Data Processors in Third Countries (2021/914/EC), hereunder updates thereto ("SCC"), are entered into before the transfers are taking place. In the case of Controller's consent to the Data Processor's use of Sub-Processors located in a Third Country, the Data Controller hereby authorizes and instructs the Data Processor to enter into SCC on its behalf."

12. General Terms

12.1 **Confidentiality.** Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("**Confidential Information**") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:
(a) disclosure is required by law;
(b) the relevant information is already in the public domain.

12.2 **Notices.** All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post, or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of Norway.

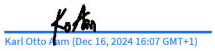
13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the Oslo District Court.

Confidential. All rights reserved to Skytech Control

14. Signatures

This Data Processing Agreement is signed digitally by both parties.

For the Data Processor



Karl-Otto Aam

CTO

For the Data Controller



Adam Eskdale Moen

IT-sjef

Confidential. All rights reserved to Skytech Control

APPENDIX 1 – SPECIFICATION OF PROCESSING OF COMPANY PERSONAL DATA

1. REFERENCE TO AGREEMENT

The Parties have on signed date concluded a Service Contract for provision of various IT services ("**Agreement**").

2. PARTIES

2.1. Introduction

The parties (individually referred to as "**Party**" and jointly referred to as "**the Parties**") to this Data Processing Agreement are as set out below and in the corresponding Agreement.

2.2. Data Controller

The Data Controller is Kragerø Kommune ("**The Data Controller**"), General public administration

Company organisation number: 963 946 902

Located at:

Pb. 128

3791 Kragerø

Norway

Contact person: Adam Eskdale Moen

Contact email: adam.moen@kragero.kommune.no

Contact phone: 99205726

Data Processor

The Data Processor is Skytech Control AS ("**The Data Processor**"), supplier of cost-, user- and asset management services.

Company organisation number: 922 607 923

Located at: Stortingsgata 4, 0161 Oslo, Norway

Contact person: Karl Otto Aam

Contact email: karlotto.aam@skytechcontrol.io

Contact phone: +47 92686945

Confidential. All rights reserved to Skytech Control

3. DATA SUBJECTS

The Company Personal Data processed in accordance with this agreement concern the following categories of Data Subjects:

- Company / organization
- Department / section
- Leader (department/section)
- Employee

4. CATEGORIES OF PERSONAL DATA

The Company Personal Data to be transferred concern the following categories of data:

- Basic contact information (not exhaustive):
    - Name
    - Phone number
    - Email address
    - Employee ID
    - Company / organization and department / section affiliation

5. SPECIAL CATEGORIES OF PERSONAL DATA (IF APPLICABLE)

The Company Personal Data transferred concern the following special categories of data:

- Not applicable

6. PURPOSE OF THE DATA PROCESSING

Pursuant to the Agreement, The Data Processor provides cost-, user- and asset management.
In this context, Data Processor particularly provides:

- Mobile and tech cost control, management, and reporting
- Wage deduction reports and online cost approval
- Employee on- and off boarding with mobile subscription porting

Asset management

- User device lease (online shop)

7. PROCESSING OPERATIONS

The Company Personal Data transferred will be subject to the following basic processing activities:

- Import and storage if mobile cost data from 3rd party (mobile service supplier)
- Import, revision, management, and storage of basic personal contact data from Data Controller or by manual input
- Creation (in-system) and storage of wage deduction information and related data and communication
- Creation (in-system) and storage of device / asset data, - purchase and order information

Confidential. All rights reserved to Skytech Control

8. DATA SUB-PROCESSORS LOCATED IN EU/EEA (IF APPLICABLE):

- Øvestad Consulting AS, (Org NO: 913 682 556), Norway (One consultant)
- Semantics AS, (Org NO: 917 439 230), Norway (One consultant)
- MAGDALENA KOZŁOWSKA, (Org: NIP / VAT ID 9721308129), Poland (One consultant)
- Intility AS (Org NO: 981967070), Norway (end-to-end ICT operational service)
- CIGEN SOLUTIONS SP. ZO.O. (VAT: PL7010937278), Poland (Consultants)

9. DATA SUB-PROCESSORS LOCATED OUTSIDE EU/EEA (SPECIFY COUNTRY AND LAWFUL BASIS FOR TRANSFER) (IF APPLICABLE):

None

10. PURPOSE AND PROCESSING OPERATIONS OF EACH DATA SUB-PROCESSOR (IF APPLICABLE):

Same as main Data Processor, all done main Data Processor systems infrastructure.

Confidential. All rights reserved to Skytech Control

APPENDIX 2 – DATA PROCESSOR'S INFORMATION SECURITY MEASURES

Skytech Control AS have compiled a general documentation to describe security measures and routines, as well as compliance with storage, for further details regarding security measures and GDPR compliancy, we would like to refer to the following documents (that should be included as attachments to this DPA):

- Data Protection Policy – Skytech Control

Skytech Control AS also have a general documentation describing default retention policy.

- Data Retention Policy – Skytech Control

Confidential. All rights reserved to Skytech Control

APPENDIX 3 – APPLICABLE LEGAL BASIS FOR TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

https://eur-lex.europa.eu/eli/reg/2016/679/oj (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Confidential. All rights reserved to Skytech Control

DATA PROTECTION POLICY

Document overview	
Document owner	Skytech Control Data Protection Officers
Decision makers	The board of directors
Valid until	Further notice
Summary	The policy is applicable to all business entities in Skytech Control Group structure. This policy sets out the overall rules for Skytech Control's handling of personal data. This policy and all instructions and routines deriving from this policy shall be documented and available for all employees.
Purpose	This policy shall form the basis of data protection and processing of personal data within Skytech Control and all subsidiaries.
Ground	https://eur-lex.europa.eu/eli/reg/2016/679/oj (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/
Updates	This policy shall be updated if updates are made in Data Protection Guideline or if it is otherwise necessary due to law.

Version history			
Date	Version	Description	Name
18.12.22	1.0	Policy decided. New template established.	Karl Otto Aam (CTO)
03.05.23	1.1	Revised	Karl Otto Aam (CTO)
07.05.24	1.2	Revised	Karl Otto Aam (CTO)
22.05.24	1.3	Revised	Karl Otto Aam (CTO)
01.10.24	1.4	Revised. Amended Section 6 and 9	Karl Otto Aam (CTO)

Confidential. All rights reserved to Skytech Control

Table of Contents

1. Summary 5
2. Introduction to Data Protection 5
3. Scope of the Policy 5
4. Principles and structure 5
5. Personal data 5
   5.1. Data protection framework 6
   5.2. Data protection awareness 6
   5.3. Main principles of processing personal data 6
   5.4. Data transfers 7
   5.5. Data protection risk assessment 7
   5.6. Privacy by design and by default 7
   5.7. Retention 7
6. Cloud platform and data storage 8
7. Organizational structure 8
   7.1. The Skytech Control organization 8
   7.2. Data Protection Officers 9
8. Declaration of commitment of employees and data protection training 9
   8.1. Information and access to data 9
   8.2. Record of processing activities 9
   8.3. Additional data and IT security regulations 10
   8.4. Reporting 10
9. Contact persons 10

Confidential. All rights reserved to Skytech Control

Definitions

"consent"	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them;
"data controller"	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, the Company is the data controller of all personal data relating to <<insert type(s) of data subject, e.g. staff, customers, business contacts etc.>> used in our business for our commercial purposes;
"data processor"	means a natural or legal person or organisation which processes personal data on behalf of a data controller;
"data subject"	means a living, identified, or identifiable natural person about whom the Company holds personal data;
"EEA"	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway;
"personal data"	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject;
"personal data breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
"processing"	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring,

Confidential. All rights reserved to Skytech Control

storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

The Rights of Data Subjects

GDPR sets out the following key rights applicable to data subjects:

- The right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure (also known as the 'right to be forgotten');
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights with respect to automated decision-making and profiling.

Confidential. All rights reserved to Skytech Control

1. SUMMARY

This policy provides a general overview of the requirements to be taken into account by all subsidiaries within the Business entity - Skytech Control including its affiliates.

This Data Protection Policy (the "Policy") defines minimum standards for the **"processing"** of **"personal data"** and assigns roles and responsibilities to stakeholders, namely the management of the Business entity, data protection officers ("DPO").

2. INTRODUCTION TO DATA PROTECTION

The term data protection refers to laws and regulations imposed by countries to ensure that personal data defined hereinafter is collected, made available, and otherwise processed in a fair and lawful manner only.

Data protection laws prohibit the processing of certain categories of personal data other than in exceptional circumstances and set out prerequisites which must be fulfilled for the processing of personal data to be lawful.

In addition to the general guidelines set out herein, all employees who process personal data should follow detailed requirements in local data protection laws, as applicable.

3. SCOPE OF THE POLICY

All Business entity's employees (including temporary employees), executives and service providers, processing personal data on business entity premises or who connect to or use any of business entity's information processing systems or devices containing personal data are obliged to adhere to this Policy.

4. PRINCIPLES AND STRUCTURE

Infringement of the applicable data protection laws and regulations may cause serious damage to Skytech Control business entity and its partners.

Hence, the Business entity's business success is highly dependent on the successful protection of personal data of customers, potential customers, business partners and employees. Therefore, data protection is critical to the Business entity's business success, future competitiveness, and viability.

5. PERSONAL DATA

If not otherwise defined by the applicable data protection laws and regulations "personal data" shall mean any information, directly or indirectly, relating to an identified or identifiable natural person (**"data subject"**). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data require special protection and treatment. As such, the confidentiality, integrity, and availability of personal data must be preserved and protected from any misuse.

Confidential. All rights reserved to Skytech Control

Unless a legitimate purpose can be established in accordance with law, personal data may not be processed. Special categories of data (see below in section 5.3) are subject to specific rules and measures appropriate to the risks and freedoms of natural persons.

5.1. Data protection framework

This Policy defines the fundamental framework for establishing, monitoring, and maintaining data protection within the business entities. The processing of personal data shall be compliant with applicable law, regulations, and this Policy.

5.2. Data protection awareness

For the Data Protection Organization to be effective, an awareness and understanding of the importance of data protection by every person who process personal data on behalf of the Business entity is crucial.

Therefore, the management of each Business entity has the duty to promote the importance of data protection to each person dealing with personal data, for example by offering adequate data protection training and education to relevant staff members. This should include, inter alia, those processing (or responsible for) personal data on behalf of the Business entity, its customers and suppliers.

5.3. Main principles of processing personal data

The following principles shall apply to data processing activities that are subject to the General Data Protection Regulation (”GDPR”) conducted by or on behalf of any entity within Skytech Control.

Personal data shall be:

- processed in compliance with applicable law, fairly and in a transparent manner in relation to the data subject. “Processing of personal data” is any operation which is performed on personal data including but not limited to collection, storage, or erasure,
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes,
- adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed,
- accurate,
- retained and destroyed according to retention polices,
- processed in a manner that ensures appropriate security of the personal data.

Data security aspects are covered within the Skytech Control´s Information Security Management (ISMS) policies and implemented in each entity.

There are different types of processing of personal data which are permissible under the applicable regulations. Where required by applicable law collection of personal data shall be based on the **“consent”** of the data subject. Consent from a data subject whose personal data is being processed shall be unambiguous, explicit, and possible to revoke by the natural person in question. Pre-ticked boxes are not valid as a basis for consent. Due to the fact that the consent will include withdrawal functionality for data subjects it should be used very restrictive, i.e. only if necessary.

Confidential. All rights reserved to Skytech Control

"Special categories of personal data" are (i) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, (ii) genetic and biometric data, and (iii) data concerning natural person´s health or sexual orientation. The aforementioned special categories of personal data shall not be collected and processed unless such collection or processing necessary and lawful under applicable law.

Upon request by data subjects, the Business entity shall provide information regarding personal data in accordance with the requirements of the applicable law, regulations, and this Policy.

All Skytech Control entities must in a clear and understandable manner inform its clients and other data subjects on the business entity's processing activities.

5.4. Data transfers

Personal data may only be disclosed to third parties (including the legal entities within the Business entity) when a legitimate basis for doing so has been established, and only provided that appropriate measures have been taken, such as signature of a Data Processing Agreement **("DPA").**

Intragroup data transfers of personal data shall be based on a legitimate interest and conducted in accordance with the applicable regulations. The participating legal entities within the Business entity shall clearly define mutual rights and obligations.

Any transfer of personal data from the EU to a country or an organization outside of the EU (including intragroup transfers) shall comply with the requirements for third country transfers set out in the GDPR and any contractual obligations imposed by clients for whom the Business entity acts as a **"data processor".**

5.5. Data protection risk assessment

To optimize time and resources, the Business entity shall focus their compliance activities in the areas of greatest risk. The risk assessment shall include the criticality of the personal data and the probability of **"personal data breach"** (unauthorized or unlawful processing, accidental loss, destruction, or damage) and the respective financial and reputational impact.

5.6. Privacy by design and by default

Each new service or business process introduced within the Business entity that processes personal data should be designed to take the protection of such data into consideration, which includes to ensure that necessary information security measures are built into its design (privacy by design). Information security is only one part of privacy by design. The remaining parts can be approximated by GDPR's principles for processing personal data, such as data minimization and purpose limitation.

Each such new service or business process should further be designed to ensure that, by default, only personal data which is necessary for each specific purpose of the processing are processed and accessible (privacy by default).

5.7. Retention

Personal data should only be stored for as long as is necessary for the purposes for which it is processed or as required by applicable law. When the retention period of personal data has expired, it

Confidential. All rights reserved to Skytech Control

should be erased or anonymized in a permanent and secure way according to Skytech Control's data retention policy.

6. CLOUD PLATFORM AND DATA STORAGE

Our data protection leverages MS Azure to ensure top-tier data, application, and information security. Data is securely geo-located in Norway (NO East) and Amsterdam (EU North), with built-in fail-over and load-balancing mechanisms. We employ advanced disaster recovery (DR) strategies, perform systematic backups, and clearly define roles and responsibilities to guarantee data integrity, availability, and resilience.

7. ORGANIZATIONAL STRUCTURE

The following roles and functions shall be implemented in order to establish an appropriate level of data protection within Skytech Control and the Business entity. Additional roles or functions may be required if stipulated by the respective applicable local law.

7.1. The Skytech Control organization

To monitor the Skytech Controls data protection status and initiate corresponding measures, the Board of Directors in Skytech Control requests an annual Skytech Control Group data protection report consisting of information covering the main data protection issues and risks of Skytech Control.

The management of the Business entities is accountable for ensuring an appropriate level of data protection.

The management enables the implementation of an adequate data protection organization. This organization if stipulated by the respective applicable law in each respective country – data protection officers ("DPO"). The management of the Business entity and its Business Units shall designate the DPO and ensure that the DPO or their respective supervisors:

- are involved, properly and in a timely manner, in all issues which relate to the protection of personal data
- are provided with resources necessary to carry out those tasks and to maintain his or her knowledge
- obtain access to personal data processing operations
- may directly report to the highest level of management of the respective Business Unit
- are bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with the respective law

The DPO can fulfil other tasks, duties, and line functions, provided that the DPO shall not be subject to conflicts of interests.

The DPO may be designated for a group of entities within one Business Unit within one country, if not affecting pre-existing legally obligatory designations.

Business entities for which the processing of personal data is not part of the core business and Business entity's which are publicly listed may designate a Business entity specific DPO in order to provide a consolidated report to the Board of Directors. The processing of personal data forms part of

Confidential. All rights reserved to Skytech Control

the core business, if the Business entity and its Business Units process consumer data on their own behalf (B2C business) or process personal data on behalf of other organizations (data processing within B2B business models) regularly.

7.2. Data Protection Officers

Each legal entity within the Business entity shall designate a DPO to coordinate all data protection issues within each entity.

The DPO is responsible for monitoring internal data protection. This includes compliance with the relevant data protection regulations.

- The following is included:
- monitoring processes for compliance with legal basis and the designated purpose;
- safeguarding the data subject's right to notification, information, correction, restriction, and erasure of the data;
- training employees in data protection and ensuring their obligation to observe data protection regulations;
- support of local management when conducting a data protection impact assessment pursuant to Article 35 GDPR;
- monitoring of technical/organizational measures for data security;

8. DECLARATION OF COMMITMENT OF EMPLOYEES AND DATA PROTECTION TRAINING

All employees within the Business entity are required to sign a data protection and non-disclosure agreement together with the employment contract, or in a separate letter. Employees who are bound to data secrecy includes temporary employees, trainees, fixed-term employees, and outworkers. The declaration of commitment will be kept together with the personnel file. If temporary staff are employed, it must be ensured that they are adequately bound to the same obligations. Data secrecy shall continue to apply after the end of the employment.

Each DPO within the Business entity provides adequate training appropriate to employee responsibility. The purpose of the training is to make the employee aware of data protection issues. The training will be repeated semi-annually. If the data protection requirements change significantly, additional training related specifically to the event will be provided.

8.1. Information and access to data

Upon request, a data subject must be provided with information about what data is stored about him/her, to whom these data have been passed on, and for what purpose(s) the data is stored.

Requests must be forwarded to a DPO without due delay'. The DPO must provide an answer in a timely manner. The DPO can assign these tasks to another person/department within the Business entity if formulated in a written procedure.

8.2. Record of processing activities

The DPO support local management when keeping a record of all processing activities in the company. The record documents the methods used for processing personal data.

Confidential. All rights reserved to Skytech Control

The processing activities on which the record is based must be documented in a reporting template and updated as needed by the respective departments which use these activities.

8.3. Additional data and IT security regulations

Managers and employees must ensure that their tasks can be carried out by a substitute in the event of unforeseen circumstances. This means that joint access rights to the necessary data and IT systems must be set up. In the absence of such access authorization, in an emergency only the system administrator in coordination with the HR department and the works council (or the management representative) is allowed to provide an authorized person designated by the local management with access to the necessary data.

Data carriers and devices on which data are stored must sent to the relevant local IT department for proper disposal. Paper is placed in specific recycling containers.

8.4. Reporting

The following data protection issues must be reported ad hoc by the management of Business entity entities to their designated DPO:

- Infringement of the applicable data protection regulation or this Policy
- Fines by public data protection authorities
- Envisaged audits/assessments by public data protection authorities
- The following data protection violations must be reported ad hoc by the DPO to the CEO:
- Infringement of the applicable data protection regulation or this Policy which might result in major financial or reputational risks
- Fines by public data protection authorities
- the DPO must provide the CEO with information required for the annual Skytech Control data protection report.

9. CONTACT PERSONS

- Magnus Ottosen, DPO for Norway – magnus.ottosen@skytechcontrol.io
- Jannica Lehtonen , DPO for Finland - jannica.lehtonen@skytechcontrol.io
- Karl Samuelsson, DPO for Sweden - karl.samuelsson@skytechcontrol.io
- Ben Hammersley, DPO for UK - Ben.Hammersley@skytechcontrol.io
- Erik Nilsen Hertzberg, DPO for Denmark - erik.hertzberg@skytechcontrol.io

Confidential. All rights reserved to Skytech Control

DATA RETENTION POLICY

Document overview	
Document owner	Skytech Control Data Protection Officers
Decision makers	The board of directors
Valid until	Further notice
Summary	The policy is applicable to all business entities in Skytech Control Group structure. This policy sets out the overall rules for Skytech Control's handling of personal data. This policy and all instructions and routines deriving from this policy shall be documented and available for all employees.
Purpose	This policy shall form the basis of data protection and processing of personal data within Skytech Control and all subsidiaries.
Ground	https://eur-lex.europa.eu/eli/reg/2016/679/oj (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
Updates	This policy shall be updated if updates are made in Data Protection Guideline or if it is otherwise necessary due to law.

Version history			
Date	Version	Description	Name
18.12.22	1.0	Policy decided. New template established.	Karl Otto Aam (CTO)
03.05.23	1.1	Revised	Karl Otto Aam (CTO)
22.05.24	1.2	Revised	Karl Otto Aam (CTO)
01.10.24	1.4	Revised. Amended Section 4	Karl Otto Aam (CTO)

Confidential. All rights reserved to Skytech Control

Table of Contents

1. Summary 3
2. Scope 3
3. Reasons for Data Retention 3
4. Data Duplication 3
5. Retention Requirements 3
6. Data Destruction 4

Confidential. All rights reserved to Skytech Control

1. SUMMARY

Skytech Control seeks to ensure that it retains only data necessary to effectively conduct its program activities and work in fulfilment of its mission.

The need to retain data varies widely with the type of data and the purpose for which it was collected. Skytech Control strives to ensure that data is only retained for the period necessary to fulfil the purpose for which it was collected and is fully deleted when no longer required. This policy sets forth Skytech Control's guidelines on data retention and is to be consistently applied throughout the organization.

2. SCOPE

This policy covers all data collected by Skytech Control and stored on Skytech Control owned or leased systems and media, regardless of location. It applies to both data collected and held electronically (including photographs, video and audio recordings) and data that is collected and held as hard copy or paper files. The need to retain certain information may be mandated by federal or local law, federal regulations and legitimate business purposes, as well as the EU General Data Protection Regulation (GDPR).

3. REASONS FOR DATA RETENTION

Skytech Control retains only that data that is necessary to effectively conduct its program activities, fulfill its mission and comply with applicable laws and regulations.

Reasons for data retention include:

- Providing an ongoing service to the data subject (e.g. sending a newsletter, publication or ongoing program updates to an individual, ongoing training or participation in Skytech Control's programs, processing of employee payroll and other benefits)
- Other regulatory requirements
- Security incident or other investigation
- Intellectual property preservation
- Litigation

4. DATA DUPLICATION

Skytech Control seeks to avoid duplication in data storage whenever possible. However, due to high availability and co-location requirements it is necessary to store information in two specific locations - Norway (NO East) and Amsterdam (EU North). This policy applies to all data in Skytech Control's possession, including duplicate copies of data.

5. RETENTION REQUIREMENTS

Skytech Control has set the following guidelines for retaining all personal data as defined in the Institute's data privacy policy.

- Website visitor data will be retained as long as necessary to provide the service requested/initiated through the Skytech Control website.

Confidential. All rights reserved to Skytech Control

- Contributor data will be retained for the year in which the individual has contributed and then for [Duration] after the date of the last contribution. Financial information will not be retained longer than is necessary to process a single transaction.
- Event participant data will be retained for the period of the event, including any follow up activities, such as the distribution of reports, plus a period of [Duration];
- Program participant data (including sign in sheets) will be retained for the duration of the grant agreement that financed the program plus any additional time required under the terms of the grant agreement.
- Personal data of subgrantees, subcontractors and vendors will be kept for the duration of the contract or agreement.
- Employee data will be held for the duration of employment and according to the 7.5.3 in Skytech Control Quality Manual V1.3.
- Data associated with employee wages, leave and pension shall be held according to the 7.5.3 in Skytech Control Quality Manual V1.3.
- Recruitment data, including interview notes of unsuccessful applicants, will be held according to the 7.5.3 in Skytech Control Quality Manual V1.3.
- Consultant (both paid and pro bono) data will be held for the duration of the consulting contract and then according to the 7.5.3 in Skytech Control Quality Manual V1.3.
- Board member data will be held for the duration of service on the Board and then according to the 7.5.3 in Skytech Control Quality Manual V1.3.
- Data associated with tax payments (including payroll, corporate and VAT) will be held according to the 7.5.3 in Skytech Control Quality Manual V1.3.
- Operational data related to program proposals, reporting and program management will be held will be held according to the 7.5.3 in Skytech Control Quality Manual V1.3.

6. DATA DESTRUCTION

Data destruction ensures that Skytech Control manages the data it controls and processes it in an efficient and responsible manner. When the retention period for the data as outlined above expires, Skytech Control will actively destroy the data covered by this policy. If an individual believes that there exists a legitimate business reason why certain data should not be destroyed at the end of a retention period, he or she should identify this data to his/her supervisor and provide information as to why the data should not be destroyed. Any exceptions to this data retention policy must be approved by Skytech Control's data protection offer in consultation with legal counsel. In rare circumstances, a litigation hold may be issued by legal counsel prohibiting the destruction of certain documents. A litigation hold remains in effect until released by legal counsel and prohibits the destruction of data subject to the hold.

Confidential. All rights reserved to Skytech Control

Document Control

Revision History:

Version Number	Date	Author	Description
0.1	13.11.23	Karl Otto Aam (CTO)	Document creation
0.2	15.11.23	Karl Otto Aam (CTO)	Document drafted
0.3	21.11.23	Karl Otto Aam (CTO)	Minor adjustments
0.4	10.01.24	Karl Otto Aam (CTO)	Minor adjustments
1.0	15.01.24	Karl Otto Aam (CTO)	Approved. Master version
1.1	20.06.24	Karl Otto Aam (CTO)	Revised.

1. SLA

This Service Level Agreement (SLA) defines the commitments and expectations regarding the accessibility of Skytech Controls' web applications and platform provided to customer . It establishes a mutual understanding between Skytech Controls and Customer, outlining the agreed-upon service levels, the measures to be implemented, and the compensations available if the uptime does not meet the defined standards.

1.1. Purpose

The purpose of this SLA is to specify the level of service on the deliverables to which Skytech Controls commits. This ensures a common understanding of the quality expectations attached to the services. The SLA also outlines the measures to be implemented and the level of an eventually compensation if the quality of service does not meet the defined expectations, including detailed provisions for uptime and availability of Skytech Controls' web applications.

1.2. Scope

The SLA defines the service level for the Skytech Controls web applications and platform provided. This SLA specifically covers the technical accessibility of Skytech Control web applications. It ensures that Skytech Control are accessible during the Agreed Service Hours.

1.3. Error reception

All types of operational disruptions must be reported to Skytech's support center. Other contact methods are not covered by the SLA agreement.

Operational failures must be reported by email:

Operation center email (08.00 – 16.00, Monday to Friday)	kundeservice@skytechcontrol.io
Operation center phone (08.00 – 16.00, Monday to Friday)	+47 920 84 444

1.4. Response time

Response time means the time it takes before Skytech Control can provide a qualified answer to the inquiry. Receipt of the inquiry is normally confirmed immediately by Skytech Control between Mon-Fri 08.00 – 16.00.

Deviation classes and times for started error correction as well as initial feedback:

Deviation class	Consequence of deviations	Started error correction	First feedback
Critical	Loss of the service that blocks the access to Skytech Controls web-applications	1 hour	30 minutes
Serious error	Reduced availability of the service or limited access to Skytech Controls web-applications	2 hours	4 hours
Less serious	Individual errors or omissions that are not immediately critical or serious to the experience and access to Skytech Controls web-applications	1 day	2 days

The deviation classes and times described above do not include situations that fall under Force Majeure as defined in the Partnership Agreement.

Response time (first feedback) for error handling is the time from when an error has been reported until Skytech has ascertained an error and has reported back to whom reported the error. An error can be experienced as a total loss of service or degraded performance or a problem using the service. Skytech Control classifies errors in three deviation classes and this means that the exact deviation class must be assessed individually for the individual error situation.

1.5. Customer is responsible for the following

Ensure that the general use for operating personnel in the operating situation of the service takes place in a secure manner, such as taking good care of user access information so that unauthorized persons do not obtain it.
Assist Skytech with troubleshooting and give a good description of the error situation.

1.6. Cost in connection with errors outside Skytech Controls area of responsibility

Customer will be charged at current rates if it turns out that the operational problem is due to mistakes made by customer.

Measurement of uptime and reimbursement

Uptime – refers to the total time during which Skytech Controls' web applications are accessible to users, excluding any Excluded time - is measured from the first to the last day of each month, and is reset every month.

There are two different time intervals that are measured:

1) Monday - Friday 08:00-17:00 CET
2) Monday – Thursday 17:00-08:00 CET + Friday 17:00 – Monday 08:00

Skytech Control shall manage the services with the resources that can ensure that the customer achieves the agreed uptime measured over a calendar month (30 days). Average uptime is measured according to the following formula:

Uptime guarantee (%) = (100 * (Number of minutes in the calendar month minus any Excluded time) Minus minutes Downtime) divided by the number of minutes in the calendar month minus any Excluded time

Uptime guarantee	95 %
Refund in case of loss / Critical error	10% of monthly cost for using Skytech Control in the relevant period
95% - 93% availability	
Refund in case of loss / Critical error	15% of monthly cost for using Skytech Control in the relevant period
92,9% - 90% availability	
Refund in case of loss / Critical error	20% of monthly cost for using Skytech Control in the relevant period
Less than 90% availability	

Excluded time = Excluded time refers to events that will not be considered downtime in the calculation of uptime. These events include, but are not limited to:

- Scheduled Maintenance Periods: Maintenance activities that occur within the predefined service window, as communicated in advance to the Customer.
- Customer configuration Errors: Issues caused by incorrect configurations, settings, or actions taken by the Customer.
- Third-Party Integration Errors: Problems arising from external services or integrations that are not managed or controlled by Skytech Controls.
- Force Majeure Events: Extraordinary circumstances beyond Skytech Controls' control, such as natural disasters, acts of terrorism, or other unforeseen events.

These exclusions ensure that uptime calculations accurately reflect Skytech Controls' performance without penalizing for situations outside of its control.