Data- og informasjonssikkerhetspolicy
Sodvin AS

Dette dokumentet angir mål og prinsipper for data- og informasjonssikkerhet knyttet til aktiviteter i regi av selskapet. Bestemmelsene i dette dokumentet bygger på selskapets virksomhetsstrategi og revideres jevnlig for å sikre samsvar med gjeldende lover og forskrifter samt eventuelle særskilte kontrakter som kan ha betydning for innholdet i dokumentet.

Dokumentet angir overordnede prinsipper for spesifikke sikringstiltak, prosedyrer og instrukser knyttet til data- og informasjonssikkerhet.

Dokumentet tillates kommunisert til eksterne i tilknytning til kontraktsforhandlinger, avtalerevisjoner og lignende situasjoner. Dokumentet er i slike sammenhenger overført i konfidensialitet og tillates ikke kopiert eller videresendt.

Spørsmål angående dokumentets innhold eller anvendelse kan rettes til:

Sodvin AS
Trondheimsveien 7C
7200 Kyrksæterøra
Support.it@sodvin.no
org nr.: 983 474 594

1. PRINSIPPER FOR DATA- OG INFORMASJONSSIKKERHET I SODVIN AS

1.1 DEFINISJONER

1.1.1 Informasjonssikkerhet

Nivå for beskyttelse av spesifikk informasjon mot ødeleggelse, utilsiktet endring, uautorisert tilgang, utpressing, ulovlig bruk og skadelig bruk.

1.1.2 Datasikkerhet

Nivå for teknisk sikring av datasystemer.

1.2 PRINSIPPER

Sodvin legger en rekke prinsipper til grunn ved etablering av nye tjenester, endring og kontroll av eksisterende tjenester og utbedring av eventuelle avdekkede sikkerhetsbrudd. Prinsippene dekker også interaksjon med kunder og sluttbrukere samt ansettelse, opplæring, instruering og oppfølging av eget personale.

Prinsipper for data- og informasjonssikkerhet i Sodvin AS:

1. All drift og leveranse av tjenester og behandling av data skal foregå i samsvar med norsk lov
2. Løsninger og arbeidsmetoder skal følge retningslinjer i iSO27001/2 der dette er relevant.
3. Ingen kunder skal kunne se andre kunders data eller systemer
4. All brukertilgang skal være autorisert gjennom personlig påloggingskode og personlig passord. I enkelttilfelle kan interaktiv tilgang til enkelte funksjoner tillates gjennom upersonlig pålogging. Dette kan gjelde spesielle terminalfunksjoner som betalingskasse, lagerscanner o.l. Funksjonspåloggingskoder skal være låst til fysisk enhet gjennom bruk av MAC ID eller annen unik identifikator
5. Alle systemer og dataområder som inneholder eller kan inneholde sensitive personopplysninger, eller opplysninger om straffbare forhold knyttet til personer, skal beskyttes med minst to-faktor autentisering, som f.eks. både personlig påloggingskode, personlig passord, og personlig token i form av mobiltelefon, Bank-ID, Buypass-ID eller tilsvarende
6. Ingen lagringssystemer eller sentrale produksjonsservere skal være direkte tilknyttet offentlig nett. Slike systemer skal være koblet gjennom Proxy-server som igjen skal være koblet gjennom adekvat brannveggløsning
7. Alle produksjonsdata skal sikres gjennom adekvate backupløsninger. De sikkerhetskopierte dataene skal også være lagret på annet geografisk sted.
8. Tilbakekopiering / rekonstruksjon av tapte data skal være dokumentert, og testes jevnlig
9. Kunden skal kunne tilbys krypterte datalagringsløsninger der dette er påkrevd eller ønsket
10. Brukergrensesnitt skal være publisert gjennom sikre løsninger som krypterer alle overførte data.
11. Alt driftspersonell og andre som får utvidet tilgang til systemene, skal være underlagt oppdatert og signert sikkerhetsinstruks og taushetsløfte
12. Sentrale driftsmidler skal være fysiske plassert i sikre miljøer med sikker strømforsyning, miljøkontroll og adgangskontroll. All fysisk adgang skal loggføres skriftlig eller elektronisk. Alle relevante avvik i fysiske driftsparametere eller sikringstiltak, skal avviksbehandles, og legges til grunn for vurdering av mulige forbedringstiltak

2. MÅL FOR DATA- OG INFORMASJONSSIKKERHETSARBEIDET I SODVIN AS

Selskapet har gjennom implementering av prinsippene og bestemmelsene i dette dokumentet, som mål at ingen spesifikke kundedata eller personopplysninger skal tapes, bli gjort utilgjengelige eller komme uvedkomne i hende som følge av svakheter i selskapets tekniske løsninger og leveransekanaler eller som følge av aktiviteter utført av personer som opererer under selskapets ansvar.

Sodvin har følgende konkrete mål for informasjonssikkerhet:

1. Ingen hendelser, uansett årsak skal kunne føre til ugjenkallelig tap av data
2. Avvik eller brudd uten tap av tilgang til fasiliteter skal være fullt gjenopprettet innen 24 timer
3. Avvik eller brudd som omfatter tap av tilgang til fasiliteter skal være fullt gjenopprettet innen 72 timer
4. Uautorisert tilgang til data skal ikke forekomme. Avdekking av situasjoner der det har forekommet uautorisert tilgang til data, skal avviksbehandles. Korrektive tiltak skal være iverksatt og testet innen 24 timer
5. Innbrudd i egne lokaler eller tyveri av stasjonært eller mobilt datautstyr, enten fra egne lokaler, eller i ansattes varetekt, skal ikke kunne gi delinkventen direkte eller indirekte tilgang til hverken selskapets egne, eller kunders data.

3. PERSONOPPLYSNINGER UNDER BEHANDLING AV SODVIN AS

All behandling av personopplysninger i Sodvin søkes utført i tråd med vår personvernpolicy (se eget dokument).

3.1 PERSONOPPLYSNINGER OVERFØRT DIREKTE FRA KUNDE TIL SODVIN AS

Følgende personopplysninger er obligatoriske for hver enkelt sluttbruker, og overføres direkte til Sodvin AS ved etablering av brukertjenester:

- Fullt navn
- Personlig e-post adresse
- Oppstartsdato for de aktuelle tjenestene
- Stoppdato for avbestilte tjenester

Følgende personopplysninger er anbefalt overført. Manglende opplysning kan medføre redusert tjenestetilgang eller tilgang til supporttjenester

- Mobiltelefon
- Rolle / Stilling

Se også egen personvernerklæring.

3.1.1 Behandling av personopplysningene

Opplysningene registreres i Sodvins service og supportsystem, Connectwise og Hubspot. Opplysningene knyttes til følgende andre opplysninger:

- Kundeorganisasjon (de som har rekvirert tjenestetilgangen)
- Tjenestetilganger
- Ansvarsområder i forhold til avtaler og kontrakter
- Personlig datautstyr under driftsavtale med Sodvin

3.1.2 Bruk av personopplysningene

De registrerte opplysningene benyttes til følgende formål, hvorav samtlige er knyttet til overliggende tjenesteavtaler:

- Sluttbrukers personlige e-post adresse benyttes til brukeridentifisering og tilgangsstyring og kobles enten alene eller sammen med brukers fulle navn til de forskjellige underliggende sikkerhetssystemer. Alle tilganger er knyttet mot kundeorganisasjon som overliggende objekt.
- Sluttbrukers personlige e-post benyttes til å koble mottatte supporthenvendelser mot sluttbruker som kontaktperson.
- Sluttbrukers e-post og mobiltelefon Benyttes ved respons på innmeldte saker og henvendelser
- Sluttbrukers e-postadresse/adresser benyttes for konfigurering av e-postsystem for brukere med e-post gjennom Microsoft / Hosted Exchange.

Sodvin AS benytter ingen av de overførte personopplysningene til egne formål.

3.1.3 Overføring av personopplysninger

Sodvin overfører ikke mottatte personopplysninger til 3.part utenfor selskapets kontroll. Overføring av enkelte personopplysninger forekommer ved produksjon av flere av tjenestene levert gjennom Sodvin. All slik overføring er kontrollert og utført av personell direkte tilknyttet Sodvin, og underlagt selskapets datainstruks og taushetserklæring. Vedlagt finnes oversikter over de enkelte overføringene, hvordan de behandles, og hvilke underliggende avtaleformer som regulerer overføringene. I utgangspunktet forekommer det ingen interaksjon med ekstern 3.partsorganisasjon i produksjon og drift av slike tjenester, og ingen eksterne er autorisert for tilgang til de overførte personopplysningene. Se eventuelle vedlagte oversikter for ytterligere informasjon.

3.2 PERSONOPPLYSNINGER OVERFØRT INDIREKTE AV KUNDE TIL SODVIN AS GJENNOM KUNDENS BRUK AV AVTALTE TJENESTER

Sodvin AS er i utgangspunktet ikke kjent med omfang og karakter av kundeorganisasjoners innsamling, registrering og bruk av personopplysninger i de tjenester som leveres gjennom Sodvin. I forbindelse med ny EU/EØS lov om vern av personopplysninger (GDPR), som tredde i kraft 25.05.2018, vil Sodvin søke å innhente informasjon om omfang og karakter av slik behandling fra alle som benytter våre tjenester, for å danne et grunnlag for å vurdere vår sikkerhetsarkitektur opp mot kundens tjenestebruk, kunne gi råd til kunden om utforming av databehandleravtale, og, om nødvendig, kunne etablere ekstra sikringstiltak.

3.3 PERSONOPPLYSNINGER REGISTRERT GJENNOM VÅRE NETTSIDER

Enkeltpersoner kan registrere seg gjennom våre nettsider for å motta vårt nyhetsbrev eller for å komme i kontakt med oss for mer informasjon om våre tjenester. Opplysninger oppgitt i disse sammenhengene behandles strengt i samsvar med personopplysningsloven. Se ellers egen personvernerklæring på https://www.sodvin.no

4. GENERELT OM SODVINS BEHANDLING AV KUNDENS DATA

Kundens produserte og lagrede data behandles rutinemessig slik, uavhengig av innholdets karakter og omfang:

1. Lagringsområde for kundens dokumenter og filer er kun tilgjengelig for sluttbrukere under kundens kontroll. Eventuell ytterligere tilgangsstyring gjøres kun etter instruks fra kundeorganisasjonen

2. Privat e-postboks og private dokumentområder er kun tilgjengelig for den personen som eier e-post adressen/påloggingsprofilen

3. SQL databaser settes opp etter spesifikasjon fra kundens systemleverandør(er). Sodvin utfører aldri operasjoner som medfører innsyn i innhold i SQL baser uten direkte instruks fra kundeorganisasjon

4. Alle produksjonsdata lagres på redundante disksystemer

5. GENERELT OM SIKKERHETSARKITEKTUR I SODVIN TJENESTEPRODUKSJON

5.1 FYSISK SIKRING AV SENTRALE DRIFTSMIDLER

Alle fysiske komponenter eiet eller direkte kontrollert av Sodvin, og som inngår i verdikjeden for produksjon og leveranse og drift av tjenester levert av Sodvin, er plassert i egnede datasenter med begrenset tilgang, sikring av strøm og temperatur og relevante varslingssystemer ved avvik. Unntak fra dette er lokale nettverksenheter eller endepunktsutstyr som f.eks. PC, router, brannvegger og andre nettverkskomponenter som er utplassert i kundens lokaler. Fysisk sikring av slike enheter er overlatt aktuell sluttkunde. Det er p.t. ikke stilt spesifikke krav til fysisk sikring av slikt utstyr.

5.2 FYSISK OG LOGISK SIKRING AV TJENESTETILGANGER

5.2.1 Passiv og aktiv sikring mot skade og avvik ved strømbrudd

Utstyr er sikret mot uønsket avbrudd grunnet bortfall av strøm med disse tiltak:

- Doble strømforsyningskurser fra hovedinntak på bygg frem til enhet
- Sentral batteribank for avbruddsfri datastrøm
- Reservegenerator for kontinuerlig drift ved lengre strømavbrudd

Det er automatisk omkobling mellom de forskjellige strømkildene. Avbrudd i hovedstrøm og unormale temperaturendringer varsles driftsvakt gjennom automatisk epost/SMS melding i tillegg til driftskonsoller. Driftsvakt er ansvarlig for oppfølging og etterkontroll.

5.2.2 Passiv og aktiv sikring av kommunikasjonslinjer mot brudd

Kommunikasjonslinjer mot offentlig nett er etablert med doble tilknytninger med separat linjeføring fra forskjellige leverandører. Det er automatisk omkobling av tjenester ved linjebrudd. Linjebrudd varsles fra linjeoperatør til driftspersonale ved SMS og e-post. Aktiv omkobling ved linjebrudd varsles driftspersonale ved automatisk e-post.

5.2.3Fysisk sikring av produksjonsdata

Som kundens produksjonsdata regnes data lagret i sentrale lagringssystemer under direkte kontroll av Sodvin AS i disse kategoriene:

- Kundens delte filområde
- Sluttbrukers private filområde
- Alle e-post lagringsområder
- Alle SQL Transaksjonsdatabaser

Data lagret på mobile enheter, lokale maskiner, bærbare PC'er m.m. under kundens/sluttbrukers kontroll er ikke sikret på spesiell måte fra Sodvin med mindre dette er spesifikt avtalt.

Standard lagringssystemer for kunders produksjonsdata er satt opp med disse aktive og passive sikringstiltakene:

- Redundante lagringssystemer med automatisk forvarsling ved degradert ytelse på enkeltelementer
- Kontinuerlig sikkerhetskopi av alle data til lagringssystem, med katastrofesikring i separat datasenter

5.2.4 Sikring mot datahacking og virusangrep

Alle perimetere er sikret med brannveggløsninger med innebygget trafikk-kontroll med bl.a.:

- Blokkering av usikre nettsteder (følger kontinuerlig oppdatert internasjonal liste)
- Monitorering av nett-trafikk for skadelig programvare
- IPS/IDS (Intrusion Prevention/ Detection System)
- DDOS angrepshindring og varsling

All e-post trafikk til/fra våre servere er scannet gjennom ekstern mailsikringstjeneste.

5.2.5 Sikring mot identitetstyveri

All aksess til tjenester og systemer levert av Sodvin autoriseres gjennom bruk av personlig ID og personlig passord. Kundene velger om de ønsker flere kontrollfaktorer. For kontroll av mottaker benyttes en kombinasjon av personlig e-post adresse og personlig mobiltelefonnummer.

5.2.6 Sikring mot feilaktig utlevering av data og opplysninger

Enhver utlevering av data og opplysninger gjøres kun etter autorisasjon av sluttkundes ansvarlige leder i henhold til kundens egen opplysning ved kontraktsinngåelse, eller ved senere endringer.

5.2.7 Sikring mot feilaktig behandling av registrerte personer

Sluttkunde er selv ansvarlig for å bestille endringer i brukertilganger. Kun medarbeidere hos sluttkunde som ved kontraktsinngåelse, eller ved senere endringer, er gitt fullmakt til bestilling av brukerendringer, har tilgang til denne tjenesten. Etter aktivering av ny bruker eller endret bruker, bekreftes endringen skriftlig til bestiller for kontroll av korrekt tilgangsoppsett og persondata.

6. UTVALGTE SKYTJENESTER

Sodvin tilbyr en rekke verdiøkende tjenester produsert utenfor Sodvins egeneide produksjonsmiljø.

6.1 MICROSOFT OFFICE365 OG AZURE

Sodvin tilbyr Microsoft Office365 som standard programpakke for Office produkter og tjenester
Tjenestene brukes under en direkte sluttbrukerlisensavtale mellom kundeorganisasjon og Microsoft. Sodvin overfører ingen av kundens data til Microsoft, utover bruk av tjenester i MS datasentre etter kundens eget valg. Enkelte av applikasjonene og tjenestene lar kunden/sluttbrukeren selv overføre data til Microsoft. Det er opp til kundeorganisasjonen selv å påse at det ikke overføres opplysninger via disse tjenestene på en måte som strider mot norsk personvernlovgivning.

Sodvin har ingen databehandleravtale mot Microsoft. Microsoft sin personvernerklæring finnes her:
https://privacy.microsoft.com/nb-no/privacystatement

Microsoft tilbyr sluttbruker et eget verktøy for å konfigurere sine personverninnstillinger her:
https://account.microsoft.com/privacy/

Kundeorganisasjon oppfordres til å etablere egne interne instrukser for bruk av skytjenestene hos Microsoft. Dersom en kundeorganisasjon finner at de av forskjellige årsaker ikke ønsker å benytte Microsoft Office365 tjenestene, kan Sodvin tilby alternative løsninger for de fleste behovene denne tjenestepakken dekker.

7. GENERELT OM RISIKOVURDERING FOR FRONTDESK® TJENESTER

Generell risikovurdering for personopplysninger behandlet gjennom FRONTDESK® tjenester er av kategori LAV. Generelt sikkerhetsnivå for standard tjenesteleveranser gjennom FRONTDESK® er MIDDELS. Sodvin har i forbindelse med innføring av ny personvernforordning (GDPR), igangsatt en tjeneste for kundens egendeklarering av registrerte personopplysninger. Sodvin tilbyr kunder som angir storskalabehandling av personopplysninger, behandling av sensitive personopplysninger eller behandling av personopplysninger som kan medføre høyere risiko for den registrerte, bistand til etablering av høyere sikkerhetsnivå, og andre tiltak for å sikre kundens organisasjon som Behandlingsansvarlig fortsatte samsvar med gjeldende Personopplysningslov.

8. KONFIDENSIALITET

Sodvin garanterer at alt personell involvert i behandling av kundeorganisasjonens data herunder overførte personopplysninger, gjennom skriftlig avtale er underlagt taushetserklæring etter straffelovens §21 og markedsføringslovens §28 og §29 og at disse gjennom instrukser, rutiner og opplæring har nødvendig kunnskap om personvern og behandling av personopplysninger.