Databehandleravtale

mellom

[KUNDE]

Behandlingsansvarlig
[ORGNUMMER KUNDE]

og

Pindena AS

Databehandler

999 183 719

1. DEFINISJONER

I Databehandleravtalen skal følgende ord og uttrykk ha denne betydning:

1. “Personopplysninger” enhver opplysning om en identifisert eller identifiserbar fysisk person (“den registrerte”); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet,
2. “Behandling” enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.
3. “Underdatabehandler/Underleverandør”: en annen databehandler eller flere (underleverandører) som Databehandler engasjerer for å utføre spesifikke behandlingsaktiviteter på vegne av Behandlingsansvarlig.
4. “GDPR”: General Data Protection Regulation. Europaparlamentets- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernloven).
5. “Gjeldende personvernregler”: gjeldende lover og regler om personvern, inkludert ny personopplysningslov og GDPR (fra og med ikrafttredelsestidspunkt).
6. “Registrerte eller Deltagere”: siden Databehandler har et påmeldingssystem, vil Behandlingsansvarlig sine kunder igjen omtales som registrerte eller deltagere.

2. FORMÅLET MED AVTALEN

1. Denne avtalen ("Databehandleravtalen") er mellom [KUNDE] (“Behandlingsansvarlig") og [Pindena AS] ("Databehandler"), der begge utgjør en "Part", samlet benevnt som "Partene".
2. Databehandleravtalens hensikt er å regulere rettigheter og plikter i henhold til Europaparlamentets- og rådsforordning (EU) 2016 av 27. april 2016 om vern av

fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, samt om oppheving av direktiv 95/46/EF (generell personvernloven/ General Data Protection Regulation).

3. Avtalen skal sikre at personopplysninger om de registrerte ikke brukes urettmessig eller kommer uberettigede i hende. Avtalen regulerer databehandlers bruk av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.
4. Databehandleravtalen regulerer Databehandlers behandling av personopplysninger på vegne av Behandlingsansvarlig i forbindelse med Hovedavtalen. Databehandleravtalen varer så lenge Hovedavtalen varer.
5. Databehandleravtalen har fire vedlegg. Vedleggene er en del av Databehandleravtalen.
   5.1. Vedlegg 1 inneholder en oversikt over godkjente underdatabehandlere.
   5.2. Vedlegg 2 inneholder en beskrivelse av tekniske og organisatoriske sikkerhetstiltak.
   5.3. Vedlegg 3 inneholder Personvernerklæring fra Pindena Påmeldingssystem.
   5.4. Vedlegg 4 inneholder dokument om Sikkerhet i Pindena Påmeldingssystem.

3. BISTAND TIL BEHANDLINGSANSVARLIG

1. Generelt
   Databehandler skal bistå Behandlingsansvarlig med å oppfylle sine forpliktelser i henhold til Gjeldende personvernregler.

2. Forespørsler fra tredjeparter
   Dersom den Registrerte, myndigheter eller andre ber om informasjon fra Databehandleren vedrørende Behandlingen av Personopplysninger i medhold av denne Databehandleravtalen, skal Databehandleren henvise forespørselen til Behandlingsansvarlig.

   Databehandleren skal ikke, uten forutgående instrukser eller godkjenning fra Behandlingsansvarlig, overføre eller på annen måte utlevere Personopplysninger eller annen informasjon knyttet til Behandlingen av Personopplysninger til en tredjepart. Hvis Databehandleren i henhold til Gjeldende personvernrett er pålagt å utlevere Personopplysninger som Databehandleren behandler på vegne av den Behandlingsansvarlige, må Databehandleren umiddelbart varsle Behandlingsansvarlig om dette.

3. Forespørsler fra de registrerte
   Databehandleren skal bistå Behandlingsansvarlig så langt det er mulig for å oppfylle Behandlingsansvarliges plikt til å besvare forespørsler fra de registrerte i henhold til *Personvernloven kapittel 3 om informasjon, innsyn, korrigering, sletting, begrenset behandling og portabilitet.* Databehandler skal gjøre personopplysningene tilgjengelige så snart som mulig.
   I den grad Databehandleren mottar slike forespørsler direkte fra de registrerte, skal Databehandleren henvise den registrerte til Behandlingsansvarlig, og deretter følge opp når forespørselen kommer fra Behandlingsansvarlig.
   Dersom pålagte frister ikke overholdes grunnet Databehandlerens manglende eller forsinkede respons innenfor vanlig arbeidstid, skal Databehandler holdes ansvarlig for dette. Her må det selvsagt informeres om i god tid om en selv har en pålagt frist.

4. Sletting
   Databehandleren kan etter forespørsel fra Behandlingsansvarlig, utføre uthenting eller sletting av Personopplysninger til standard veiledende timepris.

5. Behov for bistand
   Ved behov for bistand skal Behandlingsansvarlig sende en skriftlig henvendelse til Databehandler. Ved slik bistand skal Databehandler fakturere

Behandlingsansvarlig etter nødvendig medgått tid etter standard veiledende timepris.

4. TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

Se vedlegg 2 for mer informasjon angående tiltakene. Dette punktet baserer seg på selve handlingen, og generelt sikkerhet.

1. Databehandler skal ikke utlevere personopplysninger til tredjeparter uten skriftlig forhåndsgodkjenning fra Behandlingsansvarlig. Unntak gjelder for eventuelle godkjente underdatabehandlere (se avtalens punkt 6) når de har behov for opplysningene for å kunne utføre sine oppgaver.

2. Databehandler sikrer at kun de personer som er autorisert til å behandle personopplysninger, har tilgang til personopplysningene som behandles på vegne av Behandlingsansvarlig.

5. TAUSHETSPLIKT

1. Databehandlers ansatte og andre som opptrer på Databehandlers vegne, har taushetsplikt om informasjon og personopplysninger som vedkommende får tilgang til etter Databehandleravtalen. Taushetsplikten omfatter også ansatte hos underdatabehandler som utfører oppdrag for Databehandler for å kunne levere tjenesten.
2. Taushetsplikten gjelder også etter Databehandleravtalens opphør. Ansatte og andre som fratrer sin tjeneste hos Databehandler skal pålegges taushet også etter fratredelse om forhold som nevnt ovenfor.

6. UNDERDATABEHANDLERE

1. Godkjente underdatabehandlere er oppført i Vedlegg 1.
2. Databehandler plikter å inngå skriftlig avtale med hver underdatabehandler som regulerer underdatabehandlers behandling av personopplysninger og pålegges å ivareta alle plikter som Databehandleren selv er underlagt etter denne Databehandleravtalen.
3. Databehandler plikter å forelegge disse avtalene for Behandlingsansvarlig etter forespørsel.
4. Databehandler skal kun engasjere underdatabehandlere som gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at databehandlingen

oppfyller kravene etter gjeldende personvernregler. Databehandler skal gjennomføre revisjoner av underdatabehandlere. Databehandler skal kunne fremlegge rapporter fra slik kontroller for Behandlingsansvarlig.

7. REVISJON

1. Databehandler skal dokumentere og gjøre tilgjengelig for Behandlingsansvarlig, informasjon som er nødvendig for å påvise etterlevelse av Databehandleravtalen og gjeldende personvernregler.

2. Databehandler skal muliggjøre og bidra ved revisjoner av Databehandlers behandlingsaktiviteter som utføres av Behandlingsansvarlig eller av annen inspektør med fullmakt fra Behandlingsansvarlig. Databehandler skal også muliggjøre og bidra ved revisjoner fra tilsynsmyndigheter.

3. Databehandleren kan foreta jevnlige revisjoner av sine behandlingsaktiviteter. Dette kan Databehandler gjøre på egen hånd eller via annen inspektør med fullmakt fra Databehandler. Databehandleren skal oversende kopi av revisjonsrapporter fra slike revisjoner til Behandlingsansvarlig om de ønsker. Behandlingsansvarlig skal ha rett til å fremlegge slike revisjonsrapporter til sine eksterne revisorer og tilsynsmyndigheter.

4. Om Behandlingsansvarlig krever bruk av ekstern inspektør, må Behandlingsansvarlig selv dekke kostnader for dette.

5. Databehandleren kan utføre revisjoner av underdatabehandlere. Dette kan sendes Behandlingsansvarlig om de har bedt om en revisjon, eller ønsker å få tilsendt. Tid som medfører å utføre og holde revisjon vil bli fakturert kunden (Behandlingsansvarlig, kunde av Databehandler) pr time til standard timepris.

6. Dersom en revisjon avdekker avvik fra forpliktelsene i Databehandleravtalen, skal Databehandler så snart som mulig avhjelpe slike avvik (og, hvis relevant, påse at den relevante underdatabehandler gjør det samme). Behandlingsansvarlig kan kreve at hele eller deler av behandlingsaktivitetene midlertidig opphører til vellykket utbedring er bekreftet. Ved særlig alvorlige brudd kan Behandlingsansvarlig kreve behandlingen stoppet, opplysningene tilbakeføres til Behandlingsansvarlig og terminere Hovedavtalen samt Databehandleravtalen.

8. VARIGHET OG OPPHØR

1. Databehandleravtalen gjelder fra den er signert med begge Parters underskrift og gjelder så lenge Hovedavtalen fortsatt er i drift. Altså så lenge Behandlingsansvarlig fortsatt er i et kundeforhold med Databehandler.

2. Behandlingsansvarlig kan ved brudd på Databehandleravtalen eller bestemmelsene i gjeldende personvernlovgivning pålegge Databehandler å stoppe den videre behandlingen av personopplysningene med øyeblikkelig virkning.

3. Opphør skjer ved at Behandlingsansvarlig leverer inn oppsigelse. Partene blir da enige om en stengedato. To (2) uker etter stengedato så vil Databehandler slette installasjonen og all tilhørende informasjon.

4. Ved behov og enighet så kan Databehandler og Behandlingsansvarlig bli enige om en varighet å beholde installasjonen om det er nødvendig uten sletting. For eksempel pause i betaling grunnet COVID-19 problemer.

5. Behandlingsansvarlig kan selv hente ut data før stengedato. Om de behøver ytterligere hjelp, så kan dette kjøpes som konsulenttimer til veiledende pris pr time. Om det ønskes å hente ut data når installasjonen er stengt, men ikke slettet enda, vil dette også faktureres til veiledende timepris.

9. VERNETING

Avtalen er underlagt norsk rett og partene vedtar Tønsberg tingrett som verneting. Dette gjelder også etter opphør av avtalen.

10. KONTAKTPERSONER

Partenes kontakt etter denne avtalen, skal skje mellom følgende kontaktpersoner:

	For [Fylles ut]	**For Pindena AS**
Navn:	[Fylles ut]	Heidi Martens-Lea
Stilling:	[Fylles ut]	Key Account Manager
Tlf:	[Fylles ut]	33 80 65 06
E-post:	[Fylles ut]	heidi.martens@pindena.no

Om kontaktpersoner ikke er tilgjengelig, så skal andre personer hos hver av Partene kontaktes. Det får man vite om når man kontakter Parten.

Denne avtale er i 2 – (to) eksemplarer, hvorav partene har hvert sitt.

11. UNDERSKRIFT

Sted/dato: BY, 00.00.0000

Behandlingsansvarlig
[Fylles ut]

_____
[Fylles ut]

Sted/dato: Tønsberg, 00.00.0000

Databehandler
Pindena AS

Heidi Martens-Lea

_____
[Fylles ut av en i Pindena]

12. Vedlegg 1 Godkjente underdatabehandlere

Underdatabehandlere / tredjepart benyttet av Databehandler. Databehandler har egne Databehandleravtaler knyttet med hver av underdatabehandlere.

Bedriftsnavn	Org.nr.	Adresse	Behandling
Empatix AS	987 895 993	Bjellandveien 24, 3172 VEAR	Utvikling og design
Webhuset	981 532 484	Nygårdsgaten 114, 5008 BERGEN	Leie av virtuelle servere
Amazon Web Services Inc.		410 Terry Avenue North, Seattle, WA 98109-5210, USA.	Leie av virtuelle servere
ISP-huset	985 838 186	Arups gate 18, 3015 DRAMMEN	Domener (fusjonert med Miss Hosting)
Miss Hosting	985 838 186	Filipstad brygge 1 0252 OSLO	Domener (fusjonert med ISP-huset)
Link Mobility AS	992 434 643	Langkaia 1, 0150 OSLO	SMS utsendelse
Google LLC		1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Kan nedlaste vår QR-app
Apple's iOS App Store		Apple 1 Infinite Loop Cupertino, CA 95014-2084	Kan nedlaste vår QR-app

13. Vedlegg 2 Tekniske og organisatoriske sikkerhetstiltak

Databehandler skal som et minimum gjennomføre alle de tiltak som er angitt eller henvist til nedenfor. Databehandler kan ikke uten skriftlig samtykke fra Behandlingsansvarlig gjøre endringer i disse tiltakene som reduserer graden av datasikkerhet. Databehandler skal kontinuerlig arbeide for å forbedre sikkerhetstiltakene og sørge for at de oppdateres i takt med den teknologiske utviklingen.

13.1.1 Pseudonymiseringstiltak

Definisjon og forklaring: Pseudonymisering vil si behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsinformasjon, forutsatt at slik tilleggsinformasjon oppbevares separat og er gjenstand for tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar person.

Om det ønskes å samle inn informasjon uten at det skal knyttes til en identifiserbar person, så må det samles inn anonymt. Det mest anonyme måten er da at det ikke legges inn kontaktinformasjon som navn, mobilnummer og e-postadresse. Databehandler har ikke egne tiltak for å separere informasjon. Det er mulig å utforme skjema slik at brukere (administratorer) kan identifisere hvilke felt i skjema som er sensitiv informasjon. Dette i sammenheng med at brukere hos Behandlingsansvarlig kan sette opp innstillinger på siden for sletting av deltagere, og sensitiv informasjon fra installasjonen.

13.1.2 Krypteringstiltak

Definisjon og forklaring: Kryptering er prosessen med koding av data på en slik måte at bare autoriserte personer har tilgang til opplysningene.

I databasen så er alle data lagret i klartekst, bortsett fra passord som er kryptert. Tilgang til database er med passord, og kunnskap for å håndtere det.

13.1.3 Tiltak for å sikre personopplysningenes fortrolighet (konfidensialitet)

Definisjon og forklaring: Eksempler kan være tiltak for å kontrollere tilgang, og for å skille opplysningene fra opplysninger som Databehandler behandler på vegne av andre behandlingsansvarlige.

Kun kunden (Behandlingsansvarlig) sine ansatte som de har gitt brukere får se hva som fylles ut. Om man velger lisens Enterprise, kan man fordele både brukere og aktiviteter i ulike avdelinger, og kan dermed ha visse aktiviteter med muligens mer sensitive opplysninger skjult fra alle bortsett fra brukere som har tilgang til avdelingen. Fra Databehandler sin side, er det ansatte med taushetsplikt, som heller ikke logger seg inn med mindre det gjelder Support, oppgradering og annen hjelp.

13.1.4 Tiltak for å sikre personopplysningenes integritet

Kunden henter da selv inn informasjonen, og må selv passe på hva og hvordan dette gjøres. Databehandler overvåker ingen informasjon. Om Databehandler oppdager informasjon som er brudd på personvernloven, kan det varsles til Datatilsynet.

13.1.5 Tiltak for å sikre tilgjengeligheten til personopplysningene

Databehandler tar daglig backup av alle serverne, både filer og databaser.

13.1.6 Tiltak for å sikre robusthet i behandlingssystemene og -tjenestene

Som nevnt under punkt 13.1.5 så er det backup. Det kan dermed gjenopprettes fra backup. Det er ikke valgt redundante servere, så vi velger ikke selv lokale som serverne er i.

13.1.7 Tiltak for fysisk sikring av lokaler hvor data behandles

Databehandler sine servere i Sverige står i Stockholm, og de som er igjen i Norge står i Bergen og Oslo.

13.1.8 Andre datasikkerhetstiltak:

Databehandler har opprettet rutine for revisjon av underdatabehandlere. Dette er allerede en rett som er sikret i egne Databehandleravtaler, og vil tre i kraft hvis Databehandler eller Databehandler sine kunder skal ha ønske om å utføre revisjon. Dette er for å forsikre seg om at de følger våre Databehandleravtaler som respektive underdatabehandlere.

14. Vedlegg 3 Personvernerklæring

NB! Gjeldende Personvernerklæring i skrivende stund. Nyeste oppdatert kan finnes på følgende nettside:
https://faq.pameldingssystem.no/article/408-personvernerklaering
Følgende tekst er hentet ut 23.09.2020 kl 14:50.

- Når registrerer vi personopplysninger?:
    - Vi registrerer opplysninger når vi får henvendelser via support e-poster eller telefoner, andre henvendelser, inngår nye kundeforhold, melder seg på våre kurs og lignende.
    - Ved support henvendelser av våre kunder registreres det i vårt support e-postsystem som kalles HelpScout.
    - I nye kundeforhold samler vi inn informasjonen ved at dere fyller ut skjema. Når noen fyller ut vårt skjema for prøveløsning, blir dette registrert, og vi henter inn mer informasjon om personen om vi behøver.
- Hvilken informasjon samler vi inn fra våre kunder?:
    - Nytt kundeforhold: Her samles det inn informasjon om økonomi, grunnet at lisenser faktureres. Informasjon fylles også ut i vårt regnskapssystem, Tripletex. Her hentes ofte informasjon med organisasjonsnummer, og ellers det som den nye kunden har fylt ut i skjema.
    - IP adresser av våre brukere lagres i 14 dager.
    - Support eller andre henvendelser. Her er informasjonen som kunden selv oppgir: e-post, telefonnummer, navn, blir lagt inn i vårt CRM system (OnePageCRM) og e-postsystem.
    - Kurs: om noen melder seg på våre kurs, samles inn informasjonen de fyller ut. Navn, firma, e-post og telefonnummer.
- Hva med informasjonen sendt inn fra deltagere?:

- Våre kunder utformer selv skjema slik de selv ønsker, og samler inn informasjon som kunden selv ønsker.
- Vi gjør ikke noe med informasjonen som blir samlet inn. Våre kunder spør om informasjonen de ønsker, og informasjonen lagres.
- Pindena AS behandler denne informasjonen ved at det lagres i systemet, og dermed lagres på databaser på servere.
- Pindena AS videresender ikke til tredjepart.

- Hva bruker vi info til:
  - All informasjon om våre kunder som vi mottar ved utfylling av et av våre skjema, eller henvendelser til oss, blir som regel brukt til å kommunisere med kunden.
  - Sende ut viktig informasjon om viktig oppdateringer av systemet.
  - Sender ut invitasjoner til våre egne kurs i systemet.
  - Utsendelse av faktura i vårt regnskapssystem.
  - Bruker ikke informasjonen som samles inn av våre kunder.
- Pindena Påmeldingssystem sin nettside:
  - Samler inn cookies (informasjonskapsler)
  - Samler inn info som man fyller ut i våre skjema.

15. Vedlegg 4 Sikkerhet i Pindena

Gjeldende dokument om Sikkerhet i Pindena Påmeldingssystem; versjon 6.1.0. datert 23.09.2020.

1.Om dokumentet

Dette dokumentet beskriver hvordan sikkerhet er håndtert i Pindena Påmeldingssystem. Dokumentet beskriver nærmere sikkerhet både for klient og i koden. I tillegg til ekstra tjenester som e-post, servere, domene og personvern. Dette dokumentet er også som et vedlegg for Databehandleravtale.

1.Om dokumentet

Dette dokumentet beskriver hvordan sikkerhet er håndtert i Pindena Påmeldingssystem. Dokumentet beskriver nærmere sikkerhet både for klient og i koden. I tillegg til ekstra tjenester som e-post, servere, domene og personvern. Dette dokumentet er også som et vedlegg for Databehandleravtale.

2. Sikkerhet på klientsiden

Krypterte forbindelser og sikkerhet i programvaren på serversiden hjelper ikke hvis man har virus/trojanere eller andre sikkerhetshull på sin egen PC. Sikkerheten begynner på den siden brukeren sitter. Brukernavnet og passordet du mottar er personlig – ikke gi det til andre, og husk å endre passord etter du har logget inn.

3.Sikkerhetstiltak i koden

All programvare laget i Pindena-rammeverket har følgende sikkerhetstiltak:

3.1 Rollesikkerhet

Hver bruker kan ha null eller flere roller tilknyttet.
Rollene kontrollerer:

1. Hvilke maler brukerne kan se.
2. Hvilke menyelementer brukerne kan se.

3. Hvilke funksjoner brukerne kan utføre (klikk på knapper som endrer data etc).

3.2 Databasesikkerhet

Hver kunde har sine egne databasetabeller, som bare kundens installasjon har tilgang til.
Alle data lagres i klartekst i databasen bortsett fra passord som er kryptert.

3.3 Templatesikkerhet

Pindena Påmeldingssystem er mal-/templatebasert, og tilgang gis for hver enkelt template.

1. ”Nekt først-policy” på backend-maler. Hvis malen ikke har et definert sikkerhetsnivå har ingen tilgang til disse malene. Det er altså bevisste handlinger som må til for å tilgjengeliggjøre maler og tilgangsnivå til maler for de ønskede rollene.
2. Maler som ikke inngår i sikkerhetssystemet er som standard ikke tilgjengelige.
3. Maler i frontend har alle tilgang til, men for å utføre endringer uten pålogging så er det nødvendig med en unik ID.

3.4 Forebygge øktkapring (session hijacking)

3.4.1 Følgende er gjort for å forebygge øktkapring:

1. Session tidsavbrudd ved inaktivitet (session utløper etter en periode med inaktivitet selv om timeout ikke er nådd, og bruker blir logget ut). Antall timer er avhengig av ønsket sikkerhet. Kort utløpstid er mest sikkert.
2. Bytte av cookie-id ved pålogging for å hindre ”session fixation”.
3. Alle kunder med vårt domene har HTTPS. De med eget domene kan få HTTPS for en ekstra kostnad.

3.5 Forebygging av angrep

3.5.1 Følgende er gjort for å forebygge direkte angrep:

1. Vi bruker rammeverket Laravel som har innebygget beskyttelse mot tre typer angrep:
    a. ”SQL Injection attack”
    b. ”XSS attack” (Cross Site Scripting)
    c. “CSRF attack” (Cross-Site Request Forgery)

2. Validering av all input som skal lagres i databasen eller presenteres i en mal.
    a. All input blir konvertert til den minst sikkerhetskritiske datatypen som løser oppgaven.
    b. Input i tallfelt blir konvertert til tall.
    c. Input i datofelt blir konvertert til datoer.
    d. Tekst som ikke skal ha formatering blir konvertert til ren tekst.
    e. Siste utvei er lagring av HTML kode som vi prøver å unngå, men der vi må gjøre det blir det vasket mot svartelister for å hindre lagring av kode som kan gi sikkerhetsproblemer.

3.7 Logging

Logger brukes for sporing i tilfelle angrep. Følgende logger finnes:

1. Session-logg over brukersesjoner.
2. Logger for bruk.
3. Webserver-logg.
4. Google Analytics-logg.

Webserver logg slettes etter 14 dager.

3.8 Auditlogg

Pindena Påmeldingssystem har kraftig audit-funksjonalitet. Merk at dette genererer mye data. Audit-logging kan konfigureres på spesifikke felt i tabeller der det er av særskilt interesse å følge med på endringer.
Det som automatisk logges er:

1. Deltagerstatus
2. Betalingsstatus

Kunden kan også ønske hvilke felt som skal logges (fakturerbart).

Alle endringer i feltet blir logget og man har en historikk på alle verdier som har vært i feltet i tabellen og hvem som endret det og når de endret det.

4. E-post

Følgende tiltak er utført for å redusere risikoen for at utsendelser skal bli oppfattet som søppelpost:

1. Vår egen e-postadresse er lagt inn som en standard avsenderadresse, og kunder kan be om å endre dette om de ønsker.

2. Kunder har muligheten til å be om å sende e-poster fra egen konto i feks SendGrid, Mandrill, Mailgun og lignende epostklienter. Kunder som benytter seg av e-postklienter for utsendelse, bes følge råd om Whitelabel og andre sikre tiltak. Ved å sende fra andre klienter, så kan man se statistikk på utsendelser, samt velge egen avsenderadresse.
3. Vi anbefaler kunder om å ha færrest mulig bilder i e-post som et tiltak for å prøve å unngå spamfilter hos mottager.

5. Server

1. Pindena AS har retten til å flytte kunder mellom servere og leverandører; dette kan være nødvendig grunnet best ytelse for kunde. Med mindre annet er avtalt så kan kunder flyttes til servere som er lokalisert i andre EU/EØS land.
2. I Sverige har vi servere i Stockholm hos verdenskjente Amazon. I Norge så leier vi virtuelle servere av Webhuset AS som har sine datasentre i Oslo og Bergen. Webhuset sine servere bruker operativsystemet Debian 8 med automatisk oppdatering av sikkerhetspatcher.
3. Vi tar daglig backup av alle serverne, både filer og databaser.
4. Serverne overvåkes med Monit og varsler med både e-post og SMS ved feil.

6. Domene

Vi benytter Miss Hosting (tidligere ISP-huset) for domener. Miss Hosting holder til i Oslo.

7. Personvern

7.1 Tiltak:

1. Ingen deltagerinformasjon i kundens installasjon vil bli utgitt til tredjepart, eller brukt av Pindena.
2. Etter at en installasjon stenges, så skal den slettes etter 2 uker, med mindre annet er avtalt.
3. Innført SMS-verifisering på deltagerinformasjonsnivå.
4. Reservert felt for samtykke, med link til side for personvern.
5. La ansvarlig velge hvilke felt som er sensitiv og ikke.

6. Ansvarlig kan sette hvor lang tid informasjon skal være lagret etter aktivitetsslutt, og etter det vil det bli slettet fra Pindena Påmeldingssystem og så fra databasen.

7.2 Tiltak kunden bør gjøre overfor sine deltagere:

1. Be om godkjennelse til å innhente informasjon, ved å benytte “Samtykke” feltet med link til personvernerklæring.
2. Kun innhente informasjon som er godkjent.
3. Slette informasjonen etter en viss tid. Enten ved å slette deltager eller selve aktiviteten.
4. Slette informasjon om deltageren hvis den ønsker å bli slettet.
5. Sette opp innstillinger for å benytte Slette funksjoner for deltagerdata og sensitiv deltagerdata.
6. Si ifra til Pindena om tidligere aktiviteter skal slettes fra databasen (fakturerbart om man ikke gjør det selv).

8. Diverse

- “Min side” kan benyttes for at deltagere kan logge inn, og se hvilke aktiviteter de har deltatt i og blitt invitert til. Her kan de laste ned vedlegg som er aktuelle for aktiviteten, som: faktura, QR-kode, kursbevis og billett.
- Ved bruk av tredjeparts selskap på eget initiativ og ønske (som betalingsløsninger, e-postklienter og lignende), så er ansvaret mye til kunden selv, da Pindena ikke har valgt ut dette som egne underleverandører.
- I forbindelse med Pindena sine underleverandører, så er det opprettet Databehandleravtaler med disse. Om kunden ønsker kan de tilsendes.