Vedr. risikovurdering og informasjonssikkerhet i tjenesten sykkeldyktig.no

Utfyllende spørsmål og svar om informasjonssikkerhet for tjenesten sykkeldyktig.no som er juridisk underlagt Trygg Trafikk., se spørsmål 30.

1. Har leverandøren et styringssystem for informasjonssikkerhet (f.eks. ISO27001)?
Svar: Ikke ISO, men interne systemer i tråd med datatilsynets anbefalinger.

2. Er roller og ansvar knyttet til informasjonssikkerhet definert i organisasjonen, og er dette kommunisert til alle ansatte?
Svar: Ja

3. Har organisasjonen fastsatt sikkerhetsmål og fastsatt en strategi for å nå disse? Er målene og strategien kommunisert?
Svar: Fokus på prosess og rutiner, ikke konkrete mål

4. Har organisasjonen fastsatt et nivå for akseptabel risiko, samt utarbeidet rutiner for når en risikovurdering skal utarbeides/gjennomføres?
Svar: Risikovurdering gjøres periodisk. Se hjemmeside til Trygg Trafikk om personvern.

5. Har organisasjonen en plan for opplæring av ansatte og IT-sikkerhetspersonell?
Svar: Gjøres som del av introduksjon for nyansatte i Trygg Trafikk.

6. Har organisasjonen et avvikssystem, og er de ansatte kjent med sin plikt til å melde avvik?
Svar: Ja.

7. Gjennomfører organisasjonen systematiske revisjoner knyttet til informasjonssikkerhet?
Svar: Ja, årlig gjennomgang.

8. Finnes rutiner for endringshåndtering, hendelseshåndtering, kapasitetsovervåking?
Svar: Ja.

9. Har leverandøren en beredskapsplan for tjenesten, og er denne innøvd?
Svar: Ja, vi har normale rutiner for å overvåke status og gjenopprette tjenesten ved avbrudd. Rutinene står i forhold til tjenestene som tilbys og krav til oppetid.

10. Har leverandøren en løpende tilnærming til informasjonssikkerhet? Praktiseres for eksempel «ledelsens gjennomgang»?
Svar: Vi har en løpende tilnærming, men praktiserer ikke egne gjennomganger. Vårt syn er at det ikke nødvendig i et lite miljø, men foretar årlig gjennomgang av personvernrutiner og håndtering av data iht. databehandleravtaler.

11. Har løsningen mulighet for å avdekke sikkerhetshendelser og eventuelt misbruk av tilganger gjennom logging?
Svar: Ja, innlogginger og feil ved innlogging loggføres løpende.

Sykkeldyktig.no c/o
Trygg Trafikk, Tullinsgt. 2
0103 Oslo
post@sykkeldyktig.no

12. Har leverandøren tilstrekkelig oversikt over administratorer av systemet, og er tilgangene begrenset til et tjenstlig behov?
Svar: Ja.

13. Har løsningen støtte for sterk autentisering? Eksempelvis multifaktorautentisering og/eller ID-porten?
Svar: Ja, autentisering for brukere gjennom Feide. Systemadministratorer i Campus Inkrement har to-faktorautentisering gjennom egne klientsertifikater.

14. Har leverandøren eller underleverandører fjernaksess til løsningen? Hvis ja, er disse tilstrekkelig sikret gjennom tekniske, organisatoriske og fysiske tiltak?
Svar: Ja, driftet iht *best practice* hos Microsoft i deres Azure-miljø.

15. Krypteres lagrede data i løsningen (at rest)?
Svar: Ja.

16. Krypteres data i transport (in transit)?
Svar: Ja.

17. Krypteres passord i løsningen?
Svar: Ja, se spørsmål 15

18. Håndteres eventuelle krypteringsnøkler på en forsvarlig måte? Spesifiser.
Svar: Krypteringsnøkler håndteres sikkert av Azure Key Vault.

19. Praktiseres separasjon av oppgaves hos leverandør (separation of duties)?
Svar: Ja, i forbindelse med drift, utvikling og oppdateringer.

20. Logges endringer, kopieringer, slettinger, tilgang til data etc. i systemet?
Svar: Ja, se vedlegg

21. Har løsningen rollebasert tilgangsstyring?
Svar: Ja, se vedlegg

22. Har leverandøren fysiske sikkerhetstiltak på plass for å beskytte kommunens data? Hvis ja, hvilke?
Svar: Ja. Lagring hos Microsoft på Azure i Nederland som har flere ISO-sertifiseringer for oppbevaring, lagring og håndtering av data.

23. Er kommunens data segregert fra andre kunders data?
Svar: Kundedata er logisk separert fra hverandre på applikasjonsnivå.

24. Tar leverandøren backup av data?
Svar: Ja, se vedlegg

25. Har leverandøren beskyttelse mot tjenestenekt-angrep?
Svar: Ja

26. Benytter leverandøren en form for automatisk korrelering av sikkerhetshendelser og rapportering?
Svar: Ja, som del av Azure sitt security center

27. Har leverandøren et API (Application Programming Interface) som gjør det mulig for kommunen å hente ut data i et kjent format ved opphør av avtale, eller ved andre hendelser som krever at kommunen må flytte data til en annen leverandør eller «in-house»?
Svar: Nei, vi har ikke et api for det. Data kan eksporteres i maskinlesbart format.

28. Tilbyr tjenesten føderert pålogging, f.eks. Feide? Hvis nei, er dette planlagt innført?
Svar: Ja, feide

29. Er løsningen utviklet etter en sikker utviklingsmetodikk? Sikkerhetsoppdateres løsningen jevnlig?
Svar: Ja

30. Har leverandørens ansatte tilstrekkelig kompetanse/sertifisering/bevisstgjøring i forhold til informasjonssikkerhet og personvern?
Svar: Ja. Dette reguleres også gjennom databehandleravtale mellom sykkeldyktig.no ved/Trygg Trafikk. Sykkeldyktig.no er juridisk tilknyttet Trygg Trafikk org. nr. 970 133 410, og underlagt Trygg Trafikks personvernerklæring.
Lese mer her: https://www.tryggtrafikk.no/personvern/

31. Har leverandørens ansatte undertegnet på taushetserklæring? Gjennomføres bakgrunnssjekk ved nyansettelser?
Svar: Ja.

32. Er leverandøren villig til å signere kommunes databehandleravtale?
Svar: Ja. Sykkeldyktig.no tegner databehandleravtale med alle brukerorganisasjoner iht. regelverkets bestemmelser.

33. Har leverandøren oversikt over flyten av personopplysninger tilhørende tjenesten?
Svar: Ja.

34. Tilbyr tjenesten mulighet for den enkelte registrerte å kunne søke opp og få innsyn i sine persondata på en enkel og intuitiv måte?
Svar: Ja

35. Gir tjenesten mulighet for den registrerte til å søke opp og korrigere opplysninger om seg selv?
Svar: Ja, korrigering går via lærer og til e-læringsplattformen Campus Inkrement.

36. Gir tjenesten mulighet for den registrerte til for å slette opplysninger om seg selv?

Svar: Delvis –vi har valgt at elever som logger inn med Feide ikke kan slette egen informasjon. Det er det skolens oppgave å gjøre.

37. Gi tjenesten mulighet for dataportabilitet?
Svar: Ja, mulighet til å laste ned sin informasjon i datalesbart format.

38. Behandler tjenesten mer personopplysninger enn nødvendig for å oppfylle formålet med behandlingen?
Svar: Nei

39. Gir tjenesten mulighet for å trekke avgitte samtykker?
Svar: Ja, mulighet for å slette konti.

40. Støtter løsningen permanent/uopprettelig sletting av personopplysninger?
Svar: Ja. Sikkerhetskopier blir lagret i inntil 12 måneder, men deretter slettes alle opplysninger permanent.

41. Er løsningen utviklet etter prinsipper med innebygget personvern og personvern som standardinnstlling? (https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/)
Svar: Ja

Vedlegg 1: Sikkerhetsdokumentasjon Campus Inkrement

Sykkeldyktig.no c/o
Trygg Trafikk, Tullinsgt. 2
0103 Oslo
post@sykkeldyktig.no