Til våre kunder

Kristiansand 22. juni 2016

Norsk Interaktivs arbeid med personvern

Norsk Interaktiv har alltid hatt fokus på personvern i våre systemer. Vi vedlikeholder hele tiden våre tjenester for å opprettholde et så høyt sikkerhetsnivå for våre kunder som mulig. Den nye personvernforordningen (GDPR) innebærer derfor ikke store endringer.

I Norsk Interaktiv har vi arbeidet med å få full oversikt over den nye personvernforordningen, og hvilke endringer vi må gjøre i forhold til våre tjenester, våre prosedyrer og vår organisasjon. Vi har fått på plass all dokumentasjon, alle kontraktstillegg og alle prosedyrer dere trenger for å vise at dere/vi overholder personvernforordningen. Ny teknisk funksjonalitet er på plass i løpet av juli 2018. Nedenfor gir vi informasjon om våre tiltak samt at vi vedlegger to av de viktigste dokumentene i avtaleverket: Personvernerklæring og Databehandleravtale. Vedlagt er også vår policy angående sporing på våre nettsider.

Som leverandør av den nettbaserte læringsplattformen Mentorkit Enterprise, er Norsk Interaktiv i de aller fleste tilfeller definert som databehandler. Som databehandler behandler vi bare data på vegne av våre kunder og vi bestemmer derfor ikke formålet eller lovligheten ved behandlingen av persondata, dette er kundens ansvar. Den nye Personvernforordningen stiller mye strengere krav til alle som behandler persondata. Ønsker dere mer utfyllende informasjon om forordningen så besøk Datatilsynets nettsider.

Som en del av våre forpliktelser i forhold til personvernforordningen har vi

- Sørget for at organisatorisk og teknisk sikkerhet er på plass for alle tjenester.
- Utviklet dokumentasjonen dere trenger for å vise at dere overholder reglene, og for å informere deres brukere.
- Oppdaterte kontraktstillegg som er i samsvar med personvernforordningens krav til databehandlingsavtaler.
- Utviklet teknisk funksjonalitet for at brukere skal kunne utøve sine rettigheter som registrerte personer. Som for eksempel enkel tilgang til funksjonalitet for å be om å bli slettet fra systemet.

1 Våre tiltak

1.1 Organisatoriske tiltak

Norsk Interaktiv har implementert sikkerhetstiltakene som er fastsatt i dette tillegget, både organisatoriske og tekniske, i samsvar med gjeldende standarder. Norsk Interaktiv kan oppdatere eller justere disse sikkerhetstiltakene fra tid til annen, forutsatt at slike oppdateringer eller justeringer ikke resulterer i dårligere generell sikkerhet for tjenestene. Arbeidet med informasjonssikkerhet i Norsk Interaktiv inngår som en integrert del av de oppgaver som påhviler hver enkelt ansatt.

1.1.1 Ledelse

Ledelsen hos Norsk Interaktiv har vært aktivt involvert i å utvikle en kultur for informasjonssikkerhet i virksomheten gjennom et løpende program for bevisstgjøring. Ledelsen har årlig gjennomgang av sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene. Ledelsen kontrollerer at disse er i samsvar med virksomhetens behov og eventuelt oppdatere mål, strategi og organisering. Dette er nedfelt i våre internkontrollsystemer som inneholder rutiner for:

- risikovurdering
- sikkerhetsrevisjon
- ledelsens gjennomgang
- konfigurasjonsendring
- beredskapsplaner
- avviksbehandling

- adgangskontroll
- tilgangskontroll
- datakommunikasjon
- dokumentsikkerhet

1.1.2 Driftsadministrasjon

Det er etablert en rekke prosesser og retningslinjer basert på bransjens beste praksis, som skal sikre høyest mulig grad av konfidensialitet, tilgjengelighet og integritet i plattformen. Disse retningslinjene har strenge krav knyttet til en rekke områder, blant annet:

- Informasjonssikkerhet
- Sikkerheten til vertsmiljøet
- Tredjepartstilgang
- Kapasitetskontroll
- Endringsstyring
- Sikkerhetskopiering og gjenoppretting
- Tilgangsstyring
- Dokumentasjon
- Logger og overvåking
- Beredskap
- Release management

1.1.3 Sikkerhetsstrategi

Vår sikkerhetsstrategi innebærer følgende overordnede punkter:

- Vi har til enhver tid ha en sikkerhetsansvarlig i virksomheten.
- Uvedkommende har ikke fysisk tilgang til personopplysningene, eller utstyr disse er lagret på.
- Ved behov for prioritering, har beskyttelse av personalopplysninger høyere prioritet enn kundeopplysninger.
- Tilgangskontroll sikrer at tilgang til opplysninger om ansatte og kunder skal begrenses til de som har behov for det.
- Virksomhetens nettverk er beskyttet mot inntrengning fra eksterne nettverk med brannmur som kun slipper gjennom nødvendig datatrafikk.
- Virksomhetens nettverk er beskyttet mot bruk av uvedkommende, for eksempel ved sikring av trådløst nettverk.
- Fysisk oppbevaring og drift av hardware som benyttes i forbindelse med drift av løsningen utføres av ekstern leverandør, for tiden Evry AS, i henhold til inngått driftsavtale og databehandleravtale. Bestemmelser om IT-sikkerhet er regulert i databehandleravtalen, der leverandøren som databehandler skal sørge for nødvendig og relevant IT-sikkerhet.

1.1.4 Roller og ansvar

Alle ansatte har tydelige roller i selskapet, og gis kun tilgang til informasjon som kreves for deres spesifikke rolle. Et begrenset antall ansatte har administrativ tilgang til produksjonsmiljøet vårt, og rettighetene deres er strengt regulert og gjennomgås med faste, jevnlige mellomrom. Alle større endringer i programmet, miljøet eller maskinvaren for produksjonsmiljøet verifiseres alltid av minimum to personer.

1.1.5 Personellsikkerhet

Alt personell tilknyttet Norsk Interaktiv er pålagt å inngå en streng avtale om taushetsplikt. Alle medarbeidere er pålagt å følge selskapets retningslinjer for konfidensialitet, forretningsetikk og profesjonelle standarder. Personell som er involvert i sikring, håndtering og behandling av personopplysninger, er pålagt å fullføre opplæring i tråd med vedkommendes rolle.

1.1.6 Tilgangsstyring

Det er etablert strenge krav for alle ansatte, innleide konsulenter eller tredjeparter som ber om

tilgang til informasjonssystemene i Norsk Interaktiv. Tilgangskontrollen utføres av et autentiseringssystem.

Brukeren plikter å:

- ha administrativ godkjenning for den forespurte tilgangen
- ha sterke passord som er i overensstemmelse med bedriftens retningslinjer for passord
- endre passord med jevne mellomrom
- kunne dokumentere at tilgangen som forespørres, er nødvendig for den aktuelle oppgaven eller rollen
- sikre at enheten (PC, nettbrett, mobil) som brukes, er tilstrekkelig sikret, og låses når brukeren ikke er til stede.

1.2 Fysisk sikring

1.2.1 Våre arbeidslokaler

Alle arbeidslokalene hos Norsk Interaktiv er beskyttet med tilgangskontroller. Kun inviterte besøkende og ansatte kan komme inn i arbeidsområdet hos Norsk Interaktiv. Flere tiltak er etablert for å unngå sikkerhetsproblemer som skyldes tap eller tyveri av datautstyr.

1.2.2 Datasentre

Norsk Interaktivs bruk av partnere og leverandører reguleres av kontrakter, hvor også bestemmelser om informasjonssikkerhet inngår. Ved valg av partner eller leverandør vurderes ikke bare pris, leveringsdyktighet og leveransekvalitet, men også partneren/leverandørens mulighet for å følge opp og vedlikeholde leveransen over tid. I den grad personell hos partner eller leverandør gis adgang til utstyr eller programmer hvor sensitive personopplysninger behandles, gis tilgang til selve opplysningene eller til informasjon om sikring av slike opplysninger, har Norsk Interaktiv oversikt over hvilket personell dette gjelder.

Parter som behandler personopplysninger på vegne av Norsk Interaktiv, er å anse som virksomhetens databehandlere etter personvernforordningen art.4. Det inngås databehandleravtale med enhver som behandler personopplysninger på Norsk Interaktivs vegne. Norsk Interaktiv leier tjenester fra datasentre (for tiden Evry AS) som er separat fra våre arbeidslokaler. Tilgangen til datasentrene, som ligger i Norge, er strengt kontrollert og beskyttet for å redusere sannsynligheten for uautorisert tilgang, brann, vannskader og annen skade på det fysiske miljøet.

1.3 Tekniske tiltak

1.3.1 Systemtilgjengelighet

Norsk Interaktiv har implementert tiltak i henhold til gjeldende bransjestandarder for å sørge for at personopplysninger sikres fra utilsiktet tap eller ødeleggelse, herunder:

- infrastrukturredundans
- sikkerhetskopier lagres på et annet sted, og er tilgjengelig for gjenoppretting hvis det skulle oppstå svikt i det primære systemet
- hensiktsmessige beskyttelsesmekanismer for tjenestenekt
- personell tilgjengelig døgnet rundt, hele året for overvåkning og feilsøkning

1.3.2 Databeskyttelse

Norsk Interaktiv har implementert en rekke tiltak i henhold til gjeldende bransjestandarder for å forhindre at personopplysningene blir lest, kopiert, endret eller slettet av uautoriserte vedkommende ved transport eller oppbevaring. Slike tiltak omfatter:

- bruk av brannmurer, VPN-tjenester og krypteringsteknologier
- HTTPS-kryptering (også kjent som SSL- eller TLF-forbindelser) med sikre krypteringsnøkler
- ekstern tilgang til datasentre er beskyttet med en rekke lag med nettverkssikkerhetsløsninger
- samtlige utrangerte lagringsmedier gjennomgår fastsatte prosesser for utvisking av informasjon i tråd med retningslinjene våre for utvisking av informasjon fra disker, og loggføres med serienummer

- regelmessige sikkerhetsettersyn utføres av tredjepart minst en gang i året, inkludert inntrengningstesting. Resultatene gjøres tilgjengelig for kunder

1.3.3 Datasentre

Norsk Interaktiv bruker kun datasentre (for tiden Evry AS) med dagens høyeste teknologiske standard, med kontinuerlig overvåkning og sikkerhetspersonell på stedet 24 timer i døgnet, hele året. Datasentrene er plassert i Norge.

1.4 Systemutvikling

Norsk Interaktiv læringsplattform er basert på bransjestandard-teknologier fra anerkjente leverandører, som Microsoft, Azure, Zendesk m.fl . Systemene oppdateres jevnlig til nyeste versjon for å sikre at de nyeste sikkerhetsforbedringene implementeres. Plattformen oppdateres generelt flere ganger i kvartalet, og feilrettinger/forbedringer/ny funksjonalitet sendes ut etter kort tid basert på prioritet, etter nøye kvalitetskontroller.

Norsk Interaktiv har implementert tiltak for å minimere risikoen for å introdusere kode i plattformen som kan redusere sikkerheten eller integriteten til kundetjenestene og personopplysningene som behandles. Tiltakene omfatter:

• Regelmessig opplæring av ansatte
• Gjennomgang av kode
• Prosesser for kvalitetssikring og kvalitetssjekk av endringer før de distribueres

1.5 Sikkerhet knyttet til underbehandlere/sekundærbehandlere

Når nye sekundærbehandlere/underdatabehandlere skal brukes, utfører Norsk Interaktiv en revisjon av sikkerhets- og personvernpraksiser hos disse for å sikre at de har et sikkerhets- og personvernnivå i tråd med tilgangen deres til informasjon og omfanget av tjenestene de skal tilby. Norsk Interaktiv utfører regelmessige sikkerhetstilsyn av praksiser og leveranser fra eksisterende sekundærbehandlere/underdatabehandlere.

2 Hva kreves av dere som kunde?

I de aller fleste tilfeller er det Norsk Interaktiv som er databehandler på vegne av våre kunder som er behandlingsansvarlige. De fleste av våre kunder er allerede godt i gang med å sikre at de vil overholde personvernforordningen. Hvor mye hver kunde må gjøre for å få sørge for at organisasjonen i samsvar med de nye reglene, kommer an på type organisasjon og hvilke prosesser og retningslinjer som er på plass fra før.

2.1 Generelle krav

- Dere må dokumentere og vurdere all behandling av personopplysninger og systemene som blir brukt til dette. Dere bør definere formålet med behandlingen, og om denne behandlingen er lovlig. I henhold til personvernforordningen kan dere ikke behandle personopplysninger som ikke er nødvendig i forhold til de formålene som er definert.
- Dere må sørge for at behandlingen er organisatorisk og teknisk sikker, og kunne vise at den er det.
- Dere må vurdere interne prosesser for dataarkivering og -sikkerhet og dokumentere dem.
- Dere må sørge for at egen teknologi kan gi tilstrekkelig teknisk sikkerhet, og dokumentere det.
- Når dere bruker tjenester fra en tredjepart, som Norsk Interaktiv, til behandling av personopplysninger, må dere sikre at kravene som stilles til databehandlingen, er i samsvar med personvernforordningen.
- Dersom dere anskaffer ny teknologi som kan resultere i høy personvernrisiko, må dere utføre en risikoanalyse – en vurdering av personvernkonsekvenser. Dere er allerede kunde hos oss, og tjenestene våre i denne sammenhengen er ikke ny teknologi. Det kan være lurt å utføre en slik vurdering av personvernkonsekvenser. Den kan for eksempel være nyttig når dere skal dokumentere at dere overholder reglene.
- Brukerne (de registrerte) har sterkere rettigheter under den nye personvernforordningen. Våre kunder må ha en prosess på plass for å ta imot henvendelser fra brukerne og for å vurdere om det er

en lovlig grunn for å etterkomme hevendelsene de kommer med. I vår læringsplattform har vi utviklet funksjonalitet for å lette dette arbeidet.

Har dere spørsmål til oss så ta gjerne kontakt på firmapost@norskinteraktiv.no