# Databehandlers melding til behandlingsansvarlig om brudd på personopplysningssikkerheten

Melding i samsvar med artikkel 33 punkt 3 i personvernforordningen, jamfør personopplysningsloven.

|  |  |  |  |
| --- | --- | --- | --- |
| Rolle | Selskap | Organisasjons-nummer | Kontaktinformasjon personvernombud eller annen kontaktperson  |
| Behandlingsansvarlig | Kunde AS | 999 999 999 | Navn:Mobil:Epost: |
| Databehandler | Regnskapsfører AS | 999 999 999 | Navn:Mobil:Epost: |
| Underleverandør hos databehandler om denne er involvert i sikkerhetsbruddet | ASP/Systemleverandør AS | 999 999 999 | Navn:Mobil:Epost: |

Databehandler har den XX.XX.20XX kl. XX:XX fått kjennskap til et sikkerhetsbrudd hvor personopplysninger relatert til registrerte personer hos behandlingsansvarlig er berørt. Etter personvernforordningen er vi pliktig til å sende melding til behandlingsansvarlig om brudd på personopplysningssikkerheten. Nedenfor følger mer informasjon om sikkerhetsbruddet:

|  |  |
| --- | --- |
| **Art av brudd på personopplysningssikkerheten** | Beskriv nærmere, eksempelvis:* Personopplysninger på avveie
* Tyveri av lagringsmedia
* Mistet datalagringsenhet
* Hacking av eget IT-miljø
* Sikkerhetsbrudd hos databehandlers underleverandør
* Feilsending av epost
* Sending av ukrypterte personopplysninger utenfor eget domene.
* Eksponert database på internett
* Uautorisert tilgang innen egen organisasjon
* Uautorisert tilgang utenfor egen organisasjonen
* ..... annen art av brudd
 |
| **Kategorier registrerte berørt av bruddet på personopplysningssikkerheten** | Ikke navngi personene, men kategorier av personer, eksempelvis:* Ansatte hos behandlingsansvarlig
* Personlige kunder og personlige leverandører hos behandlingsansvarlig
* .....andre kategorier registrerte
 |
| **Antall registrerte berørt av bruddet på personopplysningssikkerheten** | Cirka antall personer som er berørt |
| **Kategorier personopplysninger eksponert i bruddet på personopplysningssikkerheten** | Kategorier personopplysninger som kan relateres til den registrerte, eksempelvis:* Navn
* Adresse
* Fødselsnummer
* Ansattnummer
* Kjønn
* Lønn
* Kjøpsadferd
* ....andre kategorier personopplysninger
 |
| **Eventuelle særlige kategorier personopplysninger eksponert****(jamfør artikkel 9 i personvernforordningen)** | Angi enten «Ikke aktuelt» eller en eller flere av de nedenfor. Listen er uttømmende.* Rase
* Etnisk opprinnelse
* Politisk oppfatning
* Religion
* Filosofisk overbevisning
* Fagforeningsmedlemskap
* Genetiske opplysninger
* Biometriske opplysninger
* Helseopplysninger
* Seksuelle forhold
* Seksuell orientering
 |
| **Antall registreringer berørt** | Cirka antall poster / transaksjoner som er eksponert ved sikkerhetsbruddet |
| **Annen relevant informasjon rundt bruddet på personopplysningssikkerheten** | Her er det mulig å legge til tilleggsinformasjon om saken. Ikke angi konkrete detaljer om personopplysninger i denne meldingen da den kan videresendes til Datatilsynet av behandlingsansvarlig.  |

Basert på kategorier registrerte og opplysninger har vi vurdert sannsynlige konsekvenser av bruddet basert på den kunnskap vi har på nåværende tidspunkt.

|  |  |
| --- | --- |
| **Sannsynlige konsekvenser for den registrerte av bruddet på personopplysningssikkerheten** | Beskrive og begrunne nærmere din egen vurdering, eksempelvis:* Ingen vesentlig konsekvens fordi..
* Ulempe for den registrerte fordi...
* Stor konsekvens for den registrerte fordi...
* Alvorlig konsekvens fordi...
 |

Basert på det oppståtte sikkerhetsbruddet, har vi med den kunnskapen vi har på nåværende tidspunkt gjennomført eller planlegger gjennomført følgende tiltak:

|  |  |
| --- | --- |
| **Gjennomførte tiltak for å håndtere bruddet på personopplysningssikkerheten** | Beskrive gjennomførte tiltak, eksempelvis: * Skifte passord på nettverket eller servere
* Utestenge uautoriserte brukere
* Tilbakekall av epost
* Politianmeldelse
* Sikre fysiske lokaler
* ...andre
 |
| **Foreslåtte tiltak videre for å håndtere bruddet på personopplysningssikkerheten** | Beskrive tiltak hvis aktuelt, eksempelvis* Ny risikoanalyse
* Sikkerhetsrevisjon
* Ekstern granskning
* Implementering av ny sikkerhetsløsning
* Forbedre fysisk sikring av lokaler
* ...andre
 |
| **Eventuelle tiltak for å begrense skadevirkningene som følge av bruddet på personopplysningssikkerheten** | Beskrive tiltak hvis aktuelt i denne saken |

**Videre aktiviteter:**

Det er behandlingsansvarlig som etter personopplysningsloven skal vurdere innrapportering til Datatilsynet og varsling til de berørte registrerte.

Varsling til Datatilsynet skal skje hvor det er risiko for fysiske personers rettigheter og friheter, og da innen 72 timer etter behandlingsansvarliges kunnskap om sikkerhetsbruddet. Rapportering skjer via datatilsynet.no.

De berørte registrerte skal varsles hvis det er høy risiko for fysiske personers rettigheter og friheter.