

IT-teknisk vejledning til Whistleblowerordningen

Whistleblowerportalens software bliver leveret af GlobaLeaks og hostes i skyen.

Der er valgt en cloud-løsning for at sikre den størst mulige sikkerhed mod hacking m.v. Metoden sikrer, at myndigheden kan kommunikere med whistlebloweren, uden at der udveksles e-mailadresse eller tilsvarende personlige data.

Flere andre godkendte og bredt anvendte whistleblowerordninger har valgt en lignende cloud-konstruktion fx GotEthcis® og LegalSys Whistleblower®

Cloud-leverandøren har truffet foranstaltninger til at sikre overholdelse af de essentielle garantier for persondataskyts.

Der er således truffet de fornødne tekniske og organisatoriske foranstaltninger mod, at personlige oplysninger, der lægges på cloud-udbyderens server, hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab eller misbruges.

Håndteringen af personlige oplysninger er underlagt kontroller og procedurer og overholder lovgivningen om behandling af persondata samt god skik inden for området. Screeningsenheden har taget kursus i GDPR.

Whistleblowerportalen lagrer ikke cookies på whistleblowerens computer, tablet eller telefon efter whistlebloweren har indsendt oplysninger, eller er logget ud, og efterfølgende har lukket sin browser, ligesom al datatransmission sker krypteret.

Hvis du indsender oplysninger til whistleblowerportalen fra en computer, der er på dit arbejdssteds netværk, eller via linket til portalen på uddannelsesstedets hjemmeside, vil dit besøg evt. blive registreret som led i den almindelige logning af brugeraktiviteter på netværket. Denne log må ikke tilgås uden lovlig grund.

Logning på det lokale netværk kan undgås ved at taste selve web-adressen <https://leaks.safewhistle.dk/#/> direkte browseren på en privat eller offentlig computer, der ikke er tilkoblet myndighedens netværk.

Den sikreste browser at anvende i den forbindelse er TOR-browseren, men det er ikke et krav for at kunne anmelde at man downloader og installerer denne browser.

Der er andre sikkerhedsfeatures, bla. to-faktorlogin for sagsbehandlerne, opdateringer og back-ups, samt underskrivelse af tavshedspligtserklæring for deltagere i Screenings – og Whistleblowerenheden.

Spørgsmål om den tekniske sikkerhed som ønskes afklaret inden evt. anmeldelse, kan rettes direkte til whistleblowerenheden via (anonym) anmeldelse på <https://leaks.safewhistle.dk/#/> eller til dpo@herningsholm.dk. (ikke-anonymt).

Screeningsenheden kan også kontaktes telefonisk på 7213 4950.