Dataskydd avseende Assessios testplattform Ascend.

En övergripande beskrivning av hur Assessio arbetar med dataskydd i testplattformen Ascend.

18-05-17

ASCEND
by ASSESSIO

Detta dokument syftar till att på ett övergripande sätt beskriva hur Assessio arbetar med dataskydd i testplattformen Ascend. I dokumentet används en rad begrepp, som Assessio har valt att använda på engelska då de är internationella termer.

Assessio tillhandahåller plattformen Ascend. Assessio utvecklar plattformen med egen personal som har gedigen kompetens inom området. Ascend är utvecklad enligt principerna för inbyggt dataskydd implementerat i arkitekturen. Detta innebär bland annat att vi arbetar med inbyggda mekanismer i IT-system till skydd för den personliga integriteten:

- Lösenord på olika nivåer
- Kryptering på olika nivåer
- Säkerhet på olika nivåer i kommunikationen till och från Ascend
- Behörighetsstyrning
- Funktioner för gallring (automatisk tex tidsinställd eller manuell)
- Loggning och logghantering

Ascend är en säker, stabil och pålitlig plattform som är utvecklad enligt ett omfattande internt regelverk, vilket lever upp till Datainspektionens krav såväl som gängse branschstandard.

Nedan följer en översikt över områden som är särskilt intressanta att belysa avseende dataskydd.

Säkerhet

Delat ansvar

Dataskydd, säkerhet och sekretess är ett delat ansvar mellan Assessio och våra kunder som använder plattformen Ascend. Ascend är en molnbaserad så kallad SaaS-lösning. Assessio tar ansvar för fysisk säkerhet av maskinvara, infrastruktur, och vår del av dataskyddet. Kunden har ansvar för de delar av systemet som åligger dem t ex att behörighet endast tilldelas relevanta medarbetare och att man på bästa sätt och i enlighet med GDPR tillämpar processer och rutiner som skyddar data.

Infrastruktur och hosting

Plattformen Ascend driftas och förvaltas inom molntjänsten Amazon Web Services (AWS). Ascend tillämpar omfattande säkerhetsfunktioner som tillhandahålls av AWS, vilket innefattar: Identity and Access management (IAM), dvs ett finmaskigt behörighetssystem, molnbaserad infrastruktur, multifaktor autentisering (MFA) för administratörer, fullständigt krypterad kommunikation, adekvata brandväggar, omfattande övervakning och loggningsfunktionalitet.

Kryptering

I Ascend krypteras såväl data i systemet som kommunikationen med Ascend. TLS (Transport Layer Security) tillämpas för dataskydd för kommunikation mellan plattform, användare och tredje partssystem, vilket innebär att all kommunikation med Ascend kräver säkra HTTPS-anslutningar. Vid lagring krypteras data enligt industrinormen AES-256-kryptering. Lösenord förvaras såsom hashed värden i enlighet med industrinormen bcrypt hashingfunktion.

Autentisering och verifiering

Autentisering och auktorisering följer branschstandard. Assessio följer högsta standard för web application security, inklusive den öppna Web Application Security Project (OWASP). Ascend vidtar löpande åtgärder för att följa med i den utvecklingen som sker.

Assessio stävar efter att efterleva ledande branschpraxis avseende autentisering, vilket bland annat inkluderar följande moment:

- Policy för starka lösenord
- Multi-factor Authentication (MFA)
- Strong session management (hantering av starka sessioner)
- Kortlivade åtkomst-tokens (access tokens)
- Skydd mot SQL injection-attacker

- Skydd mot Cross Site Scripting (XSS)-attacker
- Skydd mot Cross Site Request Forgery (CSRF)-attacker.

I en molnbaserad plattform är det av yttersta vikt att data endast är tillgängliga för de avsedda och behöriga användare. Assessio använder finmaskig åtkomstkontroll och behörighetskontroll i flera lager för att säkerställa full kontroll.

Överträdelse och övervakning

Assessio har ett flertal system med automatiserade rutiner som kontinuerligt övervakar Ascend och varnar för oönskade beteenden, såsom försök till dataintrång. Dessa innefattar, men är inte begränsade till, plattform och infrastruktur, samt intelligent detektering av hot genom avancerad händelseregistrering och analys. Assessio har också ett automatiserat notifikationssystem, vilket säkerställer en hög nivå av dataskydd.

Sekretess

Assessio har definierade rutiner och processer som säkerställer att sekretess vidmakthålls, både i systemet Ascend och funktioner som innebär manuella rutiner.

GDPR

Assessio har investerat i ett omfattande GDPR arbete, vilket har och kontinuerligt säkerställer efterlevnad av GDPR på kort- och långsikt. Assessios ledning har varit projektägare och projektet har involverat samtliga funktioner inom Assessio. Extern specialistexpertis har dessutom anlitats för att granska arbetet och säkerställa att Assessio efterlever GDPR från och med den 25 maj 2018. Assessio har utsett ett dataskyddsombud och har satt en organisation för att över tid säkerställa ständiga förbättringar inom dataskydd.

Underleverantörer

Vi arbetar med ett antal tredjeparts tjänsteleverantörer. Vi kräver att alla våra leverantörer arbetar med samma höga standard som Assessio, kontrollerar regelbundet att nödvändiga certifieringar finns och att fastställda processer efterlevs av underleverantörerna.

Tillförlitlighet

Tillgänglighet

Assessios tekniska infrastruktur erbjuder hög tillgänglighet och skalbarhet. Samtliga servar Assessio använder finns fysiskt placerade inom EU.

Kvalitet

Assessio har en intern kvalitetspolicy för kodning av plattformen Ascend. Våra kontroller säkerställer att Kvalitetspolicyn efterlevs och revideras vid behov. Kontrollerna innefattar såväl manuella som automatiska kontroller.

Prestanda

Assessio övervakar kontinuerligt prestanda av våra system. Vi har manuella och automatiserade åtgärder vid avvikelser varvid åtgärder vidtas enligt Assessios fastställda rutiner.

Incidenthantering

Vi följer en väldefinierad incidenthanteringsprocess, och har första-, andra och tredje linjens support för att säkerställa att incidenter hanteras omedelbart av korrekt nivå och av korrekt kompetens. Assessio arbetar kontinuerligt och strukturerat med återkoppling från kunder och eftersträvar att ständigt förbättra våra system i nära samverkan med våra kunder.