Databeskyttelse og sikkerhedsforanstaltninger i Customers 1st

C1st arbejder målrettet og systematisk med informationssikkerhed og databeskyttelse som en integreret del af virksomhedens compliance-struktur. Dette afsnit har til formål at dokumentere det risikobaserede grundlag for de tekniske og organisatoriske sikkerhedsforanstaltninger, der beskytter personoplysninger i vores systemer og processer.

Med afsæt i en dokumenteret lav risikoprofil og i overensstemmelse med kravene i databeskyttelsesforordningen, herunder artikel 25 og 32, har vi etableret et sikkerhedssetup, der understøtter fortrolighed, integritet og tilgængelighed.

Afsnittet skal sikre transparens omkring vores sikkerhedsniveau og samtidig tydeliggøre, hvordan vi løbende vurderer og tilpasser foranstaltningerne for at fastholde en høj standard for databeskyttelse og ansvarlig databehandling.

Behandlingssikkerhed:

Behandlingen af personoplysninger i vores virksomhed er forbundet med et lavt risikoniveau. Dette er dokumenteret og vurderet i overensstemmelse med Datatilsynets vejledning og danner grundlag for de tekniske og organisatoriske sikkerhedsforanstaltninger, vi har implementeret:

Link til vores risikovurdering

På baggrund af den lave risikovurdering vurderes det ikke nødvendigt at anvende eksterne revisionserklæringer eller certificeringsordninger, da de etablerede tekniske og organisatoriske foranstaltninger anses for tilstrækkelige og proportionale i forhold til behandlingsaktiviteterne.

Vi foretager dog løbende vurderinger af risikoniveauet og vores foranstaltningers effektivitet for at sikre, at sikkerhedsniveauet til enhver tid er passende i forhold til de konkrete behandlingsaktiviteter.

Link til vores procedure for revision

Vi efterlever kravene i både artikel 32 om behandlingssikkerhed og artikel 25 om databeskyttelse gennem design og standardindstillinger (privacy by design og by default). Det betyder, at vi arbejder systematisk med at sikre et passende sikkerhedsniveau i forhold til den konkrete risiko – og at vi integrerer databeskyttelse i alle relevante systemer og arbejdsgange fra starten.

Foranstaltningerne dækker både tekniske og organisatoriske tiltag og beskrives konkret nedenfor med fokus på, hvilke risici de adresserer. Dette sikrer gennemsigtighed og gør det muligt at relatere sikkerhedsforanstaltningerne direkte til vores løbende risikovurderinger.

1. Adgangsstyring og autorisation

C1st har etableret en streng adgangsstyring, hvor kun autoriserede medarbejdere får adgang til personoplysninger og systemer. Adgangsrettigheder tildeles efter **mindste-rettighedsprincippet**, således at den enkelte bruger kun har de nødvendige rettigheder for at udføre sine arbejdsopgaver. Dette reducerer risikoen for uautoriseret adgang og misbrug, idet rettighederne ikke skaber unødige muligheder for dataadgang. Alle brugere har unikke login-konti, og deling af konti er ikke tilladt.

For at sikre korrekt autorisation følger C1st veldefinerede procedurer for **onboarding og offboarding** af medarbejdere. Nye medarbejdere får kun adgang til de systemer og data, som deres rolle kræver, efter godkendelse af ledelsen. Tilsvarende lukkes adgange omgående ved fratrædelse eller ændring i jobfunktion, så tidligere medarbejdere eller interne skift ikke medfører ubrugt adgang. Der gennemføres også jævnlige gennemsyn af tildelte rettigheder (f.eks. hver 6.-12. måned) for at sikre, at adgangsniveauer fortsat er passende og opdaterede i forhold til medarbejdernes arbejdsopgaver.

2. Sikker håndtering af adgangsoplysninger

C1st stiller skrappe krav til sikker håndtering af adgangsoplysninger såsom passwords, krypteringsnøgler og andre legitimationsoplysninger.

For yderligere at beskytte login-oplysninger anvender C1st **to-faktor-autentifikation (2FA/MFA)** bredt. Det betyder, at ud over brugernavn og adgangskode kræves en ekstra engangskode eller anden faktor ved login til kritiske systemer. Dermed mindskes risikoen betydeligt for kompromittering, selv hvis et password skulle blive opsnappet. Alle administrative og eksternt tilgængelige tjenester er altid bag MFA som ekstra barriere.

Deling af adgangsoplysninger er strengt forbudt via politikker – hver medarbejder skal kun anvende egne legitimationsoplysninger. Adgangskoder til interne systemer håndteres med password managers og deles aldrig via usikre netværk.

3. **Sikkerhedsbevidsthed og personale**

Alle medarbejdere med adgang til data eller systemer instrueres i korrekt håndtering af personoplysninger og sikker adgang. De modtager oplæring i it-sikkerhed og kender til kravene i GDPR, herunder vigtigheden af at låse skærmen ved fravær fra arbejdsstationen og at behandle data med fortrolighed. Awareness opretholdes gennem løbende information og opfølgning.

4. Kryptering og pseudonymisering

C1st beskytter personoplysningers fortrolighed ved at anvende stærk kryptering under overførsel (data in transit). Al netværkstrafik, der indeholder persondata, sikres med moderne og anerkendte kommunikationsprotokoller såsom HTTPS og TLS (Transport Layer Security). Dette betyder, at selv hvis data opfanges under transmission, vil indholdet være utilgængeligt og uforståeligt for uvedkommende uden de nødvendige dekrypteringsnøgler.

Ved at anvende kryptering under overførsel reduceres risikoen væsentligt for uautoriseret adgang, aflytning og manipulation af data under transport mellem brugere, systemer og tjenesteudbydere. Det gælder både for trafik mellem interne komponenter og ved ekstern adgang via internettet.

Kryptering af data i transit er en eksplicit anbefalet sikkerhedsforanstaltning i henhold til artikel 32 i databeskyttelsesforordningen (GDPR), og C1st følger best practice ved løbende at sikre, at de anvendte teknologier er opdaterede og i overensstemmelse med gældende sikkerhedsstandarder. Kryptering indgår som en integreret del af vores tekniske sikringsniveau og understøtter vores generelle arbejde med fortrolighed, integritet og tilgængelighed i behandlingen af personoplysninger.

Personoplysninger er også krypteret, når de er lagret (data at rest). Det gælder databasen og dens backups, cache og fillagring som billeder, kvitteringer og uploadede filer. Krypteringsnøglerne administreres af C1st i AWS Key Management Service (KMS). Vores applikationsservere kræver TLS 1.3 ved overførsel. Medarbejdernes computere er også krypteret.

Ud over kryptering arbejder C1st også med **pseudonymisering** af data hvor det er muligt. Pseudonymisering indebærer, at identificerende oplysninger erstattes af kunstige identifikatorer eller kodes, således at personreference kræver supplerende information, der opbevares adskilt. I praksis betyder det, at vi i visse systemer erstatter f.eks. navn og kontaktoplysninger med unikke ID-numre eller hashværdier, når fuld identifikation ikke er nødvendig for behandlingen. Derved kan vi behandle eller analysere data med væsentligt lavere risiko, da direkte personhenførbarhed er fjernet uden brug af den separate nøgle. Denne tilgang lever op til GDPR's anbefaling om **"pseudonymisering af personoplysninger"** som en risikodæmpende foranstaltning.

5. Backup og genskabelse

For at sikre mod datatab har C1st en robust backup- og genskabelsesprocedure. Alle kritiske systemer og databaser bliver **automatisk sikkerhedskopieret** med jævne intervaller. Disse backups lagres krypteret på adskilte og sikrede lokationer. Vi benytter princippet om geografisk adskilte backups – f.eks. lagres cloud-backups i en anden fysisk region eller i et andet datacenter end primærsystemerne, hvilket beskytter mod lokaliserede hændelser som brand eller oversvømmelse. C1st tester jævnligt sine backup-genoprettelsesprocedurer.

6. Sikring af fjernarbejdspladser

C1st har implementeret klare foranstaltninger for at sikre datasikkerheden ved **fjernarbejde** (hjemmearbejde eller arbejde uden for kontoret). Alle medarbejdere, der arbejder eksternt, skal følge interne retningslinjer for hjemmearbejde, som bl.a. omfatter krav om et **sikkert arbejdssted**. Datatilsynet anbefaler at have klare retningslinjer for hjemmearbejde og brug af sikre forbindelser, hvilket C1st efterlever. Medarbejdere instrueres i at behandle fortrolige dokumenter forsvarligt hjemme og fx sørge for, at uvedkommende i husstanden ikke får indsigt i arbejdsrelaterede personoplysninger.

7. Systemovervågning og hændelseshåndtering

C1st har etableret en proaktiv **systemovervågning** og en klar beredskabsplan for **hændelseshåndtering** (incident response). Vi overvåger kontinuerligt vores it-infrastruktur og applikationer for tegn på uregelmæssigheder eller sikkerhedshændelser. Dette inkluderer real-time overvågning af serverbelastning, netværkstrafik og security events via intrusion detection/prevention systemer (IDS/IPS). Hvis en usædvanlig aktivitet eller et potentielt angreb registreres – f.eks. gentagne mislykkede login-forsøg, usædvanlig dataudtræk eller malware-alarm – udløses alarmer til det relevante sikkerhedspersonale med det samme.

8. Logning og stikprøvekontrol

C1st opretholder en struktureret og kontrolleret praksis for logning af systemaktiviteter med henblik på at sikre fuld sporbarhed, understøtte revisionsspor og dokumentere korrekt behandling af personoplysninger.

Der registreres centrale hændelser i systemer, hvor persondata behandles – herunder visning, ændring og sletning af oplysninger. Udvalgte kritiske administratorhandlinger, logges særskilt for at sikre fuld transparens i driften af vores it-miljø.

Logning gennemføres i overensstemmelse med relevante krav i databeskyttelsesforordningen og følger Datatilsynets anbefalinger. Logdata behandles fortroligt og anvendes som grundlag for kontrol, inspektion og sikkerhedsopfølgning.

For at logning skal have reel værdi, kombineres den med **stikprøvekontrol** og overvågning. C1st har procedurer for løbende at gennemgå logfilerne manuelt.

9. Sikkerhedsforanstaltninger ift. underdatabehandlere

Når C1st benytter underdatabehandlere (underleverandører, der behandler personoplysninger på vores vegne, f.eks. hosting-partnere eller supportleverandører), stiller vi strenge krav om samme høje sikkerhedsniveau hos disse som hos os selv. Inden en underdatabehandler engageres,

gennemgår C1st en grundig **due diligence**-proces: Vi vurderer leverandørens sikkerhedsstandarder, certificeringer (såsom ISO 27001, SOC 2) og historik ift. datasikkerhed. Kun leverandører, der kan fremvise **passende tekniske og organisatoriske foranstaltninger**, bliver godkendt. Dette afspejler GDPR's krav om, at databehandlere skal give tilstrækkelige garantier for at implementere passende sikkerhed

C1st indgår altid en skriftlig **databehandleraftale** med underdatabehandlere, jf. GDPR artikel 28. I disse aftaler forpligtes underdatabehandleren til fortrolighed og til at opretholde mindst samme sikkerhedsforanstaltninger, som vi selv anvender.

10. Brug af AI-systemer

C1st anvender i visse tilfælde **AI-systemer** (kunstig intelligens) for at forbedre vores tjenester, men vi gør det på en måde, der respekterer datasikkerhed og privatliv. Når vi udvikler eller implementerer AI-løsninger, indtænker vi **databeskyttelse fra starten** – i tråd med Datatilsynets holdning om, at overholdelse af principper som dataminimering og formålsbegrænsning er en forudsætning for ansvarlig brug af AI. Konkret betyder det, at vi kun fodrer AI-modeller med de nødvendige data, og at personhenførbare oplysninger anonymiseres eller pseudonymiseres hvis muligt, før de anvendes til træning eller analyse. Dermed reduceres risikoen for, at AI-systemet kompromitterer de registreredes privatliv.

C1st foretager **konsekvensanalyser (DPIA)**, når vi introducerer AI-baserede processer, der indebærer behandling af personoplysninger. Vi vurderer de potentielle risici ved AI'en – f.eks. risiko for bias/diskrimination, fejlagtige beslutninger eller utilsigtet videregivelse af oplysninger – og implementerer afbødende tiltag. AI-systemer overvåges og valideres løbende, således at deres output kontrolleres af mennesker inden vigtige beslutninger træffes. Vi sikrer, at der altid er **menneskelig indsigt og mulighed for intervention**, især hvis AI bruges i beslutningsstøtte vedrørende individer, for at overholde GDPR's krav om gennemsigtighed og fair behandling.

Desuden sørger C1st for, at eventuelle tredjeparts AI-tjenester (f.eks. cloud-baserede AI API'er) kun anvendes, hvis de opfylder vores databeskyttelseskrav. Vi uploader ikke personfølsomme data til eksterne AI-tjenester uden en klar databehandleraftale og sikkerhedsvurdering. Alt i alt anvender C1st AI på en **ansvarlig og sikker måde**, der både lever op til gældende databeskyttelsesregler og sikrer de registreredes rettigheder. Dette betyder, at teknologisk innovation går hånd i hånd med respekt for privatlivet og informationssikkerheden i vores organisation.

11. Beskyttelse mod angreb og sårbarheder

C1st har etableret en flerlaget sikkerhedsarkitektur for at imødegå angreb og reducere risikoen for kompromittering. Vi benytter bl.a. firewall og IP-filtrering til at beskytte både klienter og servere mod skadelig kode og uautoriseret adgang. Al trafik til vores applikationer passerer desuden en

Web Application Firewall (WAF), som filtrerer forespørgsler, før de når vores servere. Derudover anvendes intrusion detection og intrusion prevention-systemer (IDS/IPS) til at overvåge netværkstrafik og identificere eller blokere potentielt ondsindede aktiviteter.

Alle systemer og komponenter opdateres løbende, og kritiske patches installeres uden unødig forsinkelse for at sikre, at kendte sårbarheder lukkes så hurtigt som muligt. C1st gennemfører regelmæssige sårbarhedsscanninger på både systemniveau og netværk, og vi foretager efter behov penetrationstests for at identificere potentielle svagheder, der kunne udnyttes.

Denne tilgang er i tråd med Datatilsynets anbefalinger om løbende teknisk vedligehold og vurdering af systemets modstandsdygtighed mod angreb. Målet er at sikre fortrolighed, integritet og tilgængelighed i alle vores behandlingsmiljøer.

12. Sårbarhedsscanning og sikkerhedstest

For at opdage og udbedre sikkerhedssårbarheder, før de bliver udnyttet, gennemfører C1st regelmæssige scanninger og test af vores systemer. Vi anvender automatiserede værktøjer til sårbarhedsscanning på både netværk, servere og applikationer. Scanningerne identificerer kendte sårbarheder, fx manglende opdateringer eller uhensigtsmæssige konfigurationer, hvorefter vi foretager en teknisk vurdering og udbedrer forholdene.

Der gennemføres desuden sikkerhedstest i forbindelse med udvikling og drift. I udvalgte tilfælde foretages penetrationstest for at identificere potentielle svagheder, der ikke opdages af automatiserede værktøjer. Fokus er at forebygge kompromittering og sikre, at vi lever op til kravene i GDPR artikel 32 om passende sikkerhed.

13. Dataminimering og begrænset opbevaring

C1st efterlever nøje princippet om **dataminimering** – vi indsamler og behandler kun personoplysninger, der er relevante og nødvendige for det angivne formål. Allerede ved design af nye systemer eller processer vurderes, hvilke datafelter der reelt behøves, og unødvendige data indsamles ikke. Dette reducerer vores risikoprofil betydeligt, da færre gemte oplysninger betyder mindre følsomt indhold, der potentielt kan kompromitteres. Datatilsynet har pointeret, at overholdelse af centrale principper som dataminimering og formålsbegrænsning er en forudsætning for tillid og compliance, og C1st har indarbejdet dette i alle sine arbejdsgange.

Udover minimeret indsamling praktiserer C1st **begrænset opbevaring** (storage limitation). Vi har klare politikker for opbevaringsperioder for alle kategorier af persondata.

14. Sikring af fysiske lokaliteter

C1st værner om fysisk sikkerhed i kontorfaciliteter for at forhindre uautoriseret adgang til systemer og data. Fysisk adgang er begrænset til autoriserede medarbejdere, og der anvendes adgangskontrol i form af elektroniske nøglekort og sikre låsesystemer. Nøglekort kræves for at få adgang til bygningen uden for almindelig åbningstid, og ikke alle medarbejdere har denne adgang.

Medarbejdere er instrueret i at sikre fysisk datasikkerhed – herunder at låse deres skærm, når de forlader deres arbejdsplads, og undgå at efterlade følsomme dokumenter frit fremme.

Datatilsynet fremhæver traditionelle sikkerhedsforanstaltninger som døre, låse og adgangsbegrænsning som relevante tiltag i forhold til fysisk adgangskontrol, og C1st har netop etableret robuste låsesystemer og kontrolleret adgang til relevante lokaler.

15. Kontrol med ændringer og systemopdateringer

C1st har etableret en struktureret proces for ændringsstyring, der sikrer, at systemopdateringer og konfigurationsændringer gennemføres kontrolleret og med fokus på sikkerhed. Ændringer foretages kun efter forudgående evaluering og godkendelse, og vi vurderer løbende, om en ændring kan påvirke eksisterende sikkerhedsforanstaltninger eller adgangsrettigheder.

Systemændringer foretages i overensstemmelse med interne procedurer, hvor potentielle konsekvenser for persondatasikkerhed indgår som et vurderingskriterium. Hvis fx en komponent i systemet udskiftes, sikres det, at tidligere sikkerhedsindstillinger, rettigheder og adgangsbegrænsninger bevares.

Systemopdateringer (patches) vurderes efter kritikalitet. Kritiske opdateringer installeres hurtigst muligt efter udgivelse, mens øvrige opdateringer implementeres i planlagte vedligeholdelsesvinduer. Alle ændringer dokumenteres og kan spores. Dette bidrager til at opretholde fortrolighed, integritet og tilgængelighed i overensstemmelse med artikel 32 i GDPR.

16. Hosting og høj tilgængelighed

C1st's tjenester er hostet på en **sikker og stabil infrastruktur** med høj tilgængelighed for øje. Vi benytter en anerkendt hostingpartner/cloud-udbyder AWS, der tilbyder datacentre med robuste fysiske og miljømæssige kontroller (døgnbemanding, redundant strøm, brandbekæmpelsessystemer osv.). Ved at lægge vores systemer i professionelle datacentre opnår vi en høj baseline-sikkerhed og **oppetids-SLA**, som det ville være svært at replikere on-premise. Vores hostingmiljø er designet til at sikre vedvarende **tilgængelighed og robusthed** i systemerne, jf. GDPR artikel 32, stk. 1, litra b.

Vores tjenester er distribueret over flere AWS-tilgængelighedszoner (availability zones) i samme region. Ved strømnedbrud eller anden lokal fejl vil tjenesterne forblive tilgængelige via automatisk

failover. Redundante backups på tværs af lokationer muliggør genskabelse af driften inden for få minutter.

17. Redundans og automatisk failover

C1st har etableret en højtilgængelig infrastruktur, hvor centrale systemer og data er beskyttet mod nedbrud gennem teknisk redundans og automatiske failover-mekanismer. Vores løsninger er hostet i AWS' Frankfurt-region (eu-central-1) og udnyttes i flere fysiske lokationer inden for regionen, så driften kan fortsætte selv ved fejl på en enkelt komponent eller zone.

Applikationer og databaser er designet til at kunne overtage hinandens drift uden brugerafbrydelser via load balancing og replikering. Hvis en komponent fejler, sker der automatisk failover til en sund instans. På den måde sikres kontinuitet, og nedetid reduceres til et absolut minimum.

Data lagres redundante steder – både logisk og fysisk – og infrastrukturen understøtter RAID, geo-replikering og distribuerede cloud-tjenester. Dette understøtter GDPR artikel 32 om systemernes robusthed og høj tilgængelighed.

18. Automatisk skalering og performance

For at håndtere variabel belastning og sikre stabil **performance** benytter C1st automatisk skalering i sine systemer. Vores infrastruktur er designet til dynamisk at kunne skalere op eller ned baseret på efterspørgslen. I praksis betyder det, at hvis antallet af brugere eller transaktioner stiger markant, vil der automatisk kunne tilføjes flere serverressourcer (f.eks. flere applikationsinstanser gennem en auto-scaling group i cloud-miljøet). Omvendt kan kapaciteten nedskaleres i perioder med lav belastning, hvilket også bidrager til en mere omkostningseffektiv drift uden at kompromittere beredskabet.

Automatisk skalering sikrer, at systemet altid har **tilstrækkelige ressourcer** til rådighed og at responstiderne holdes lave, selv under spidsbelastninger. Dette er ikke alene et spørgsmål om brugeroplevelse, men også om sikkerhed, da et overbelastet system potentielt kan fejle og kompromittere integritet eller tilgængelighed. For eksempel kan vi definere grænseværdier for CPU-udnyttelse, hukommelsesforbrug eller kø-længder; når disse nås, trigges opskalering. Tilsvarende overvåger vi databaser og storage I/O – hvis de er tæt på kapacitetsgrænsen, modtager driftsteamet alarmer for at øge kapacitet eller optimere ydeevnen.

En del af performance-sikringen inkluderer også regelmæssige **load tests** af systemet, hvor vi afprøver, hvordan applikationerne klarer høj belastning, og validerer at auto-skalering fungerer efter hensigten. Eventuelle flaskehalse identificeres og afhjælpes proaktivt. Forretningskritiske funktioner har ekstra fokus; vi sørger for at selv ved maksimal forventet belastning kan systemet håndtere trafikken med en sikkerhedsmargin. Ved at kombinere automatisk skalering med grundig

performance-overvågning lever C1st op til kravet om høj **tilgængelighed og robusthed**, idet pludselige stigninger i brugeraktivitet ikke bringer systemstabiliteten eller dataintegriteten i fare.

Automatisk skalering af serverkapacitet sikrer, at ydeevnen opretholdes, også under spidsbelastning. Ved fejl i én zone omdirigeres trafikken automatisk uden nedetid.

19. Dataforarbejdning i EU

C1st behandler og opbevarer personoplysninger udelukkende i EU, nærmere bestemt i AWS' datacenter i Frankfurt (eu-central-1), hvilket sikrer overholdelse af GDPR og undgår usikkerheder ved tredjelandsoverførsler.

20. Sikker dataoverførsel (data in transit)

C1st beskytter data under overførsel ved at anvende sikre og moderne kommunikationsprotokoller i overensstemmelse med gældende sikkerhedsstandarder. Al datakommunikation mellem brugere og vores systemer foregår via HTTPS og anvender stærke cipher suites med fremadrettet hemmeligholdelse (forward secrecy), som forhindrer aflytning og manipulation.

Vi deaktiverer aktivt usikre protokoller og svage krypteringsmetoder for at sikre, at kun robust og opdateret kryptering er tilladt. Kommunikation mellem interne mikrotjenester og systemkomponenter foregår enten via interne netværk uden internetadgang eller beskyttes med TLS og/eller VPN, særligt hvis data bevæger sig på tværs af netværksgrænser.

Overførsel af filer sker via sikre protokoller som SFTP eller krypterede API-forbindelser. Vi er opmærksomme på de risici, der kan være forbundet med e-mailkommunikation, og arbejder generelt for at sikre, at personoplysninger og anden fortrolig information behandles forsvarligt ved afsendelse og modtagelse af e-mail. Dette samlede setup sikrer, at personoplysninger og andre data ikke utilsigtet tilgås, ændres eller kompromitteres under transmission.

21. Audit logs og sporbarhed

C1st sikrer detaljeret sporbarhed i systemet ved at anvende centraliseret applikationslogning via Amazon CloudWatch og Sentry. Loggene omfatter specifikke API-kald, herunder interaktioner med brugergrænsefladen og programmatisk adgang via API'er. Hver logpost indeholder oplysninger om den ramte endpoint, tidspunktet for handlingen samt pseudonymiserede data om, hvilken bruger der foretog handlingen.

Al logning er struktureret med henblik på at muliggøre sporbarhed og efterlevelse af kravene i GDPR, herunder ansvarlighedsprincippet. Loggene lagres sikkert og i et format, der understøtter revision og analyse, og de behandles fortroligt, da de kan indeholde oplysninger om systemstruktur og brugeraktivitet.

22. Ingen brug af root-adgange til AWS

C1st anvender ikke root-konti til daglig drift i vores AWS-miljø. I stedet benyttes personlige brugerkonti med flerfaktorautentifikation (MFA) og passende rettighedsniveauer. Alle administrative handlinger sker via disse konti, hvilket sikrer sporbarhed og minimerer risikoen ved kompromittering af én enkelt bruger.

Root-brugeren i AWS er deaktiveret i daglig anvendelse og benyttes kun i særlige tilfælde, hvor det er nødvendigt. Alle handlinger logges i AWS CloudTrail, så det er muligt at dokumentere, hvem der har udført hvilke administrative handlinger. Dette er i overensstemmelse med principperne om mindst mulige rettigheder og styrket ansvarlighed, som anbefalet af Datatilsynet og AWS selv.

23. Kodegennemgang og sikker kodning

C1st lægger stor vægt på sikker softwareudvikling og arbejder målrettet med både manuelle og automatiserede kontroller for at sikre høj kodekvalitet og reducere sårbarheder.

Al ny kode bliver manuelt gennemgået (peer reviewed) af en erfaren udvikler, før den udrulles til produktion. Dette hjælper med at identificere fejl og sikkerhedsproblemer tidligt i udviklingsprocessen, hvilket gør dem nemmere og billigere at rette. Kodegennemgangen fokuserer især på områder som inputvalidering, korrekt håndtering af brugersessioner og beskyttelse mod typiske angreb som SQL-injection og Cross-Site Scripting (XSS).

Ud over manuelle reviews anvender C1st automatiserede værktøjer til statisk kodeanalyse, der scanner for kendte mønstre og potentielle sårbarheder. Vi holder os opdateret på OWASP's anbefalinger og tilpasser vores værktøjer og praksis derefter.

Alle kodeændringer dokumenteres, og der føres sporbarhed over, hvem der har udviklet, godkendt og implementeret ændringerne. Dette bidrager til ansvarlighed og gør det muligt at revidere kodebasens historik i forbindelse med fejlretning eller sikkerhedsinspektioner.

24. Adgang for tredjepart

For at beskytte kundedata og undgå uautoriseret adgang giver vi kun tredjepart adgang til systemet efter skriftlig instruks fra den dataansvarlige eller mod fremvisning af en gyldig fuldmagt. Vi håndterer alle adgangsanmodninger manuelt af hensyn til datasikkerheden.

Link til vores Retningslinjer for tredjepartsadgang til systemet

Senest opdateret

Dette afsnit om behandlingssikkerhed er senest opdateret 30. oktober 2026 for at afspejle den aktuelle risikovurdering, gældende lovgivning og de tekniske og organisatoriske foranstaltninger, som C1st har implementeret.