ISO/IEC 27018:2025, Informationssikkerhed, cybersikkerhed og beskyttelse af privatlivets fred: Vejledning i beskyttelse af personoplysninger (PII) i offentlige cloudtjenester i rollen som databehandler af personoplysninger (3. udgave, 2025-08)

Beskyttelse af personoplysninger (PII) i den offentlige cloud

36 krav. For denne standard findes intet akkrediteret certifikat. Udgave 07/2026.

ISO/IEC 27018 er ikke en standard for ledelsessystemer, men en vejledning med udvidede kontroller oven på ISO/IEC 27002:2022. Der findes intet selvstændigt akkrediteret certifikat efter ISO/IEC 27018. Kontrollerne optages i erklæringen om anvendelighed for et system efter ISO/IEC 27001, og certifikatet udstedes derefter efter ISO/IEC 27001 med henvisning til ISO/IEC 27018. Standarden retter sig mod leverandøren af en offentlig cloudtjeneste, der behandler personoplysninger på vegne af sine cloudkunder. En virksomhed, der alene bruger cloudtjenester, påtager sig ikke denne rolle og vurderer med fordel kravene over for sine leverandører, ikke over for sig selv. For Leanshift er denne liste derfor først og fremmest et vurderingsskema for leverandører. Hvert punkt kan stilles som spørgsmål til leverandøren og sikres gennem databehandleraftalen efter artikel 28 i GDPR. Resultatet af en sådan vurdering er en intern registrering om overensstemmelse eller en vurderingsprofil for leverandøren, ikke et certifikat. Om nummereringen: Afsnit A.2 til A.12 følger databeskyttelsesprincipperne i bilag A til standarden, punkter med numre som A.11.6 er de supplerende kontroller, der er anført der. Punkter med numre som 8.10 eller 5.34 henviser til kontroller fra ISO/IEC 27002:2022, som standarden gør specifikke for cloud. Punkter med tilføjelsen (Grundsatz), altså princip, udledes af afsnittets eget princip, hvor bilag A ikke har en selvstændig supplerende kontrol.

Virksomhed	Dato	Udfyldt af

A.2 Samtykke og valgmulighed 2

A.2.1 **Cloudleverandøren støtter cloudkunden i at opfylde de registreredes rettigheder, for eksempel indsigt, berigtigelse, sletning og indsigelse. Ansvar og frister er fastlagt i aftalen.** Dokument

Det taler for: Dokumentationen er databehandleraftalen efter artikel 28 i GDPR med en klausul om bistand ved de registreredes rettigheder, sammen med de tekniske midler i selve tjenesten: funktioner til eksport, rettelse og sletning eller en dokumenteret supportprocedure med svarfrist. Spørgsmål til leverandøren: Hvilken funktion eller hvilken proces tilbyder I, så vi kan behandle en anmodning om indsigt eller sletning inden for en måned?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.2 (Grundsatz) **Cloudkundernes personoplysninger behandles udelukkende efter kundens dokumenterede instruks. At indhente samtykke fra de registrerede er fortsat kundens opgave i rollen som dataansvarlig, og leverandøren foregriber det ikke.**

Det taler for: Dokumentationen er instruksklausulen i databehandleraftalen plus et bevis for, at leverandøren ikke gør nogen egen sekundær brug af oplysningerne, for eksempel tjenestens privatlivspolitik og produktdokumentationen. Spørgsmål til leverandøren: Behandler I vores kundedata på nogen måde uden for vores instruks, for eksempel til produktforbedring eller modeltræning?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.3 Formålets lovlighed og angivelse 2

A.3.1 **Formålet med leverandørens behandling af personoplysninger er begrænset til at levere den aftalte tjeneste og er angivet i aftalen. Der sker ingen behandling til leverandørens egne formål.** Dokument

Det taler for: Dokumentationen er databehandleraftalen med genstand, karakter, formål og varighed af behandlingen samt kategorierne af registrerede efter artikel 28, stk. 3, i GDPR. Spørgsmål til leverandøren: Send det aftalebilag, der beskriver formålet med behandlingen udtømmende. For en lille virksomhed er leverandørens standardbilag om databehandling nok, forudsat at det indeholder disse oplysninger.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.3.2 **Personoplysninger, der er betroet leverandøren, bruges ikke til reklame, markedsføring eller andre kommercielle formål hos leverandøren uden forudgående udtrykkeligt samtykke. Leveringen af tjenesten gøres ikke afhængig af et sådant samtykke.**

Det taler for: Dokumentationen er en udtrykkelig aftaleklausul, der udelukker kommerciel sekundær brug, sammen med brugsvilkårene. Spørgsmål til leverandøren: Bekræft skriftligt, at kundedata ikke bruges til reklame, profilering eller træning af AI-modeller. Mangler tilsagnet, er tjenesten uegnet til personoplysninger.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.4 Begrænset indsamling 1

A.4 (Grundskud) **Ud over de oplysninger, kunden lægger ind i tjenesten, indsamler leverandøren ikke yderligere personoplysninger til egne formål, for eksempel telemetri, brugsprofiler eller indholdsanalyse. Driftsdata og metadata, der indsamles, er angivet og begrundet.**

Det taler for: Dokumentationen er en liste over de oplysninger, tjenesten registrerer ved siden af indholdsdata (adgangslogge, telemetri, diagnosedata) med formål og opbevaringsperiode, plus et skærmbillede af den indstilling, der slår valgfri telemetri fra. Spørgsmål til leverandøren: Hvilke data om brug, telemetri og diagnostik indsamler I derudover, hvad bruger I dem til, og kan vi slå indsamlingen fra?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.5 Dataminimering 2

A.5.1 **Midlertidige filer, der opstår ved behandling af personoplysninger, for eksempel arbejdslager, caches eller tilbagerulningsjournaler, slettes sikkert inden for en fastlagt periode.**

Det taler for: Dokumentationen er en procedure for drift eller sletning med angivet opbevaringsperiode for midlertidige data, understøttet af systemkonfigurationen, for eksempel en cachetid (TTL) eller et planlagt oprydningsjob med tilhørende kørselslog. Spørgsmål til leverandøren: Efter hvor lang tid slettes caches, midlertidige filer og mellemliggende tilstande, og hvordan overvåges det?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

8.11 **Hvor drift, test eller support ikke kræver produktionsdata, er personoplysninger maskeret, pseudonymiseret eller anonymiseret. Mængden af behandlede oplysninger er begrænset til det, tjenesten faktisk har brug for.**

Det taler for: Dokumentationen er en regel om, hvilke miljøer der må se produktionsdata, plus skærmbilleder eller scripts for den maskering, der bruges i systemer til test og udvikling. Spørgsmål til leverandøren: Arbejder jeres teams for support og udvikling med produktionsdata, og i givet fald under hvilke sikringsforanstaltninger? For en lille virksomhed er en regel om, at testsystemer udelukkende kører på genererede eksempeldata, nok.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.6 Begrænset brug, opbevaring og videregivelse 3

A.6.1 **Modtager leverandøren en juridisk bindende anmodning om at videregive personoplysninger, for eksempel fra en myndighed, oplyser leverandøren cloudkunden om det på forhånd, så vidt loven tillader det.**

Det taler for: Dokumentationen er en underretningsklausul i aftalen og en intern proces for myndighedsanmodninger med en navngiven ansvarlig. Spørgsmål til leverandøren: Underretter I os, før I udleverer data, og offentliggør I en gennemsigtighedsrapport om anmodninger fra myndigheder? En aktuel gennemsigtighedsrapport er stærk dokumentation.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.6.2 **Videregiver leverandøren personoplysninger til tredjeparter, registreres hændelsen, så den kan spores: hvem der modtog oplysningerne, hvornår det skete, hvilke oplysninger der indgik, og på hvilket grundlag videregivelsen hviler.** Dokument

Det taler for: Dokumentationen er et register over videregivelser eller en sagshistorik med disse felter, også selv om det ikke indeholder poster. Et tomt, men vedligeholdt register er acceptabelt og er den praktiske vej for en lille virksomhed. Spørgsmål til leverandøren: Fører I et register over videregivelser af data, og kan vi få udtræk fra det?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

8.10 **Personoplysninger slettes, når den aftalte opbevaringsperiode udløber, eller aftalen ophører, herunder kopier i sikkerhedskopier efter deres rotationscyklus.**

Det taler for: Dokumentationen er en sletteplan med opbevaringsperioder for hver datakategori, opbevaringsperioden for sikkerhedskopier og en slettelog eller en bekræftelse på sletning. Spørgsmål til leverandøren: Hvor længe lever vores data videre i jeres sikkerhedskopier efter opsigelse, og modtager vi en skriftlig bekræftelse på sletningen?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.7 Rigtighed og kvalitet 2

A.7 (Grundskov) **Leverandøren ændrer ikke på eget initiativ de personoplysninger, der er betroet leverandøren. Rettelser og opdateringer sker udelukkende efter instruks fra cloudkunden eller gennem funktioner, som kunden selv betjener.**

Det taler for: Dokumentationen er tjenestens redigeringsfunktioner sammen med deres ændringshistorik, plus instruksklausulen i databehandleraftalen. Spørgsmål til leverandøren: Kan vi selv rette registreringer, og logges hver ændring, så den kan spores?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

8.13 **Integriteten af personoplysninger er beskyttet ved lagring, ved overførsel og ved genetablering. Der findes sikkerhedskopier, og det er testet, at de kan genetableres.**

Det taler for: Dokumentationen er konfigurationen af sikkerhedskopieringen, kontrolsum eller integritetsmekanismer og mindst en dokumenteret genetableringstest om året med dato og resultat. Spørgsmål til leverandøren: Hvor ofte tester I genetablering, og hvilken genetableringstid forpligter I jer til i serviceniveauet?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.8 Åbenhed, gennemsigtighed og oplysning 2

A.8.1 **Brugen af underdatabehandlere, der behandler personoplysninger, oplyses, inden aftalen indgås. Ændringer i listen meddeles kunden i god tid, så kunden kan gøre indsigelse eller opsige.** Dokument

Det taler for: Dokumentationen er en aktuel liste over underdatabehandlere, offentliggjort eller stillet til rådighed i aftalen, med navn, land og formålet med behandlingen, plus en regel om underretning efter artikel 28, stk. 2, i GDPR. Spørgsmål til leverandøren: Hvor finder vi jeres liste over underdatabehandlere, hvor lang tid i forvejen varsler I ændringer, og hvordan kan vi gøre indsigelse?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.8 (Grundskov) **Inden aftalen indgås, stiller leverandøren forståelig information til rådighed om, hvordan personoplysninger behandles, hvilke sikringsforanstaltninger der findes, og i hvilke jurisdiktioner behandlingen sker.**

Det taler for: Dokumentationen er privatlivspolitikken, et sikkerhedswhitepaper, en side med sikkerhedsoplysninger (trust center) og databehandleraftalen med de tekniske og organisatoriske foranstaltninger som bilag. Spørgsmål til leverandøren: Send den aktuelle liste over tekniske og organisatoriske foranstaltninger som aftalebilag, ikke kun markedsføringsmateriale.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.9 Den enkeltes inddragelse og indsigt 2

A.9 (Grundskabelon) **Tjenesten giver cloudkunden de tekniske midler til selv at behandle anmodninger om indsigt, berigtigelse og sletning fra de registrerede, for eksempel gennem funktioner til eksport, søgning og sletning.**

Det taler for: Dokumentationen er produktdokumentationen for funktionerne til eksport og sletning, understøttet af en intern prøvekørsel: en anmodning om indsigt gennemføres fra ende til anden, og tidsforbruget noteres. Spørgsmål til leverandøren: Kan vi finde, eksportere og slette alle data om en enkelt person uden jeres hjælp?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

5.34 **Kan kunden ikke selv håndtere en anmodning fra en registreret, bistår leverandøren inden for en aftalt frist. Anmodninger, som registrerede sender direkte til leverandøren, videresendes til kunden i stedet for at blive besvaret af leverandøren.**

Det taler for: Dokumentationen er den tilsvarende klausul i databehandleraftalen med en konkret svarfrist, plus en historik over supportsager som et virkeligt eksempel. Spørgsmål til leverandøren: Hvilken frist forpligter I jer til ved bistand til de registreredes rettigheder, og hvad koster det?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.10 Ansvarlighed 4

A.10.1 **Brud på sikkerheden, der omfatter personoplysninger, meddeles cloudkunden uden unødig forsinkelse med angivelse af omfang, berørte oplysninger, årsag og de trufne foranstaltninger. En underretningsproces med ansvar og frister er fastlagt.** Dokument

Det taler for: Dokumentationen er beredskabsplanen for hændelser med tilhørende eskaleringskæde, den aftalte underretningsfrist (24 til 48 timer fungerer i praksis, så kunden stadig kan overholde fristen på 72 timer efter artikel 33 i GDPR) og registreringer om tidligere hændelser eller om en øvelse. Spørgsmål til leverandøren: Inden for hvilken frist melder I en hændelse, gennem hvilken kanal, og hvilke oplysninger leverer I sammen med den?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.10.2 **Sikkerhedspolitikker, driftsprocedurer og de tilhørende registreringer opbevares i en fastlagt periode, så behandlingen kan rekonstrueres efterfølgende.** Dokument

Det taler for: Dokumentationen er en opbevaringsregel med versionshistorikken for politikkerne, for eksempel gennem et dokumentregister eller et versionsstyringssystem med godkendelsesdatoen. Spørgsmål til leverandøren: Hvor længe opbevarer I versioner af politikker og de tilhørende registreringer, og får vi adgang til dem ved en audit?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.10.3 **Der findes en fastlagt ordning for tilbagelevering, overførsel og destruktion af personoplysninger ved aftalens ophør, med angivelse af formater, frister og håndteringen af kopier.** Dokument

Det taler for: Dokumentationen er exitklausulen i databehandleraftalen plus en bekræftelse på sletning efter aftalens ophør. Spørgsmål til leverandøren: I hvilket format og inden for hvilken frist får vi vores data tilbage, hvornår destrueres alle kopier, og modtager vi en skriftlig bekræftelse?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

5.35 **Virkningen af sikringsforanstaltningerne gennemgås uafhængigt med regelmæssige intervaller, for eksempel gennem interne audits, penetrationstest eller erklæringer fra tredjepart. Resultaterne stilles til rådighed for cloudkunden i en egnet form.**

Det taler for: Dokumentationen er et ISO/IEC 27001-certifikat med en erklæring om anvendelighed, der omfatter kontrollerne fra ISO/IEC 27018, eller en SOC 2-rapport, sammen med aktuelle sammenfatninger af penetrationstest. Spørgsmål til leverandøren: Send certifikatet, dets anvendelsesområde og en bekræftelse på, at ISO/IEC 27018 er afspejlet i erklæringen om anvendelighed. Det er værd at kontrollere, om anvendelsesområdet virkelig dækker den anvendte tjeneste.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.11 Informationssikkerhed 13

A.11.1 **Alle med adgang til personoplysninger er pålagt tavshedspligt, uanset om de er ansat direkte eller tilknyttet eksternt.** Dokument

Det taler for: Dokumentationen er underskrevne fortrolighedsaftaler eller tavshedserklæringer, der fortsat gælder efter tilknytningens ophør. Spørgsmål til leverandøren: Er alle medarbejdere og leverandører med adgang til data skriftligt pålagt tavshedspligt?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.11.2 **Udskrifter og andre papirkopier med personoplysninger fremstilles kun, hvor det er strengt nødvendigt. Det tilladte omfang er fastlagt i en regel.**

Det taler for: Dokumentationen er en regel om håndtering af udskrifter, som i datacentre typisk er et generelt forbud mod at printe i områder med kundedata. Spørgsmål til leverandøren: Printes kundedata overhovedet i jeres drift, og i givet fald under hvilke betingelser?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.11.3 **Genetableringer fra sikkerhedskopier godkendes på forhånd og logges, herunder den person, der udløste genetableringen, og de berørte oplysninger.** Dokument

Det taler for: Dokumentationen er genetableringsloggen med tidsstempel, hvem der udløste den, og omfang, som regel dannet automatisk af værktøjet til sikkerhedskopiering. Spørgsmål til leverandøren: Logger I hver genetablering, og kan vi se disse logge ved en audit?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.11.4 **Lagringsmedier med personoplysninger, der forlader lokaliteterne, er beskyttet mod uautoriseret adgang og tab, som regel gennem kryptering og en transportregistrering.**

Det taler for: Dokumentationen er et bevis for kryptering (fuld mediekryptering), registreringer af transport og overdragelse samt en fortegnelse over medier. Spørgsmål til leverandøren: Forlader medier med kundedata nogensinde jeres lokaliteter, for eksempel til sikkerhedskopiering, og hvordan er de beskyttet under transporten?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.11.5 **Brugen af ukrypterede bærbare medier og enheder til personoplysninger er forbudt eller begrænset til begrundede undtagelser med dokumenteret godkendelse.**

Det taler for: Dokumentationen er en politik for flytbare medier plus teknisk håndhævelse, for eksempel gennemtvunget kryptering af enheder eller USB-porte, der er spærret gennem enhedsstyring. Spørgsmål til leverandøren: Kan medarbejdere kopiere kundedata over på ukrypterede enheder, og hvad forhindrer det teknisk?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.11.6 **Personoplysninger, der overføres over offentlige net, er krypteret. De anvendte mekanismer svarer til det aktuelle tekniske niveau.**

Det taler for: Dokumentationen er TLS-konfigurationen (aktuel protokolversion, ingen forældede krypteringsalgoritmer) og en ekstern test af konfigurationen som rapport. Praktisk for en lille virksomhed: en gratis TLS-scanning køres en gang om året, og resultatet arkiveres. Spørgsmål til leverandøren: Hvilken transportkryptering håndhæver I, og er kryptering af lagrede data aktiv?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.11.7 **Papirregistreringer med personoplysninger destrueres på en måde, der udelukker rekonstruktion.**

Det taler for: Dokumentationen er makulatorer med et tilstrækkeligt sikkerhedsniveau eller destruktionscertifikater fra en leverandør, der arbejder efter DIN 66399 eller en tilsvarende standard. Spørgsmål til leverandøren: Hvordan destruerer I papirregistreringer om kunder, og er destruktionscertifikaterne arkiveret?

○ Åbent ○ I gang ○ Opfyldt ○ Ikke relevant

Dokumentation / begrundelse

A.11.8 **Hvert bruger-id er tildelt entydigt til en enkelt person og bliver hverken genudstedt eller delt. Fælleskonti findes kun i begrundede undtagelser og med yderligere sporbarhed.**

Det taler for: Dokumentationen er en brugerliste fra identitetssystemet uden gruppekonti, sammen med reglen om, at administrativt arbejde udføres under en personlig konto. Spørgsmål til leverandøren: Arbejder jeres driftsmedarbejdere med personlige konti, og er flerfaktorgodkendelse obligatorisk?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.11.9 **Leverandøren kan til enhver tid oplyse, hvilke personer eller roller der må tilgå personoplysninger, og holder oversigten opdateret.** Dokument

Det taler for: Dokumentationen er en oversigt over adgangsrettigheder efter rolle, understøttet af en tilbagevendende gennemgang af adgange med dato og resultat. For en lille virksomhed er et halvårligt udtræk af brugerlisten med godkendelse nok. Spørgsmål til leverandøren: Hvor mange af jeres medarbejdere kan tilgå vores data, og hvor ofte gennemgår I det?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.11.10 **Brugerkonti styres gennem hele deres livscyklus: oprettelse, ændring og hurtig deaktivering ved fratrædelse eller rolleskift.**

Det taler for: Dokumentationen er en procedure for tiltrædelse og fratrædelse med en tjekliste, plus logge over deaktiverede konti med tidsstempler. Spørgsmål til leverandøren: Inden for hvilken frist inddrager I adgangen for medarbejdere, der fratræder, og hvordan dokumenterer I det?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.11.11 **Leverandørens forpligtelser til sikkerhed og databeskyttelse er fastlagt i aftalen, herunder de tekniske og organisatoriske foranstaltninger, den bindende virkning af kundens instruks og kundens ret til audit.** Dokument

Det taler for: Dokumentationen er den underskrevne databehandleraftale efter artikel 28 i GDPR med bilaget over foranstaltninger og en ret til audit eller information. Spørgsmål til leverandøren: Send den underskrevne databehandleraftale med bilag, ikke blot en henvisning til generelle brugsvilkår.

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.11.12 **Underdatabehandlere, der behandler personoplysninger, er underlagt mindst de samme forpligtelser som leverandøren selv. Udvælgelsen og den løbende overvågning af dem følger en fastlagt proces.**

Det taler for: Dokumentationen er videreførelsen af forpligtelserne i aftalerne med underdatabehandlere (artikel 28, stk. 4, i GDPR) og en leverandørvurdering med dato. Spørgsmål til leverandøren: Hvordan vurderer I jeres underdatabehandlere, og hvilken dokumentation kræver I af dem?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.11.13 **Inden lagerplads genbruges, er det sikret, at ingen data fra tidligere brugere fortsat er tilgængelige, hverken på fysiske medier eller i virtualiserede miljøer.**

Det taler for: Dokumentationen er proceduren for rensning eller overskrivning, når lagerplads frigives, registreringer om destruktion af medier og den adskillelse mellem kunder (tenants), der er beskrevet i arkitekturdokumentet. Spørgsmål til leverandøren: Hvordan sikrer I, at genbrugt lagerplads ikke indeholder restdata fra andre kunder?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.12 Overholdelse af databeskyttelse 3

A.12.1 **De lande, hvor personoplysninger lagres og behandles, er angivet og kendt af cloudkunden. Ændringer af lagringsstederne meddeles.** Dokument

Det taler for: Dokumentationen er leverandørens oversigt over lokaliteter og regioner, i aftalen eller i dokumentationen, plus et skærmbillede af regionsindstillingen for den anvendte tjeneste. Spørgsmål til leverandøren: I hvilke lande ligger vores data i hvile, fra hvilke lande tilgås de, for eksempel i support, og kan vi fastlåse regionen?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

A.12.2 **Overførsler af personoplysninger til tredjelande er kendte, begrundede og dækket af fornødne garantier.** Dokument

Det taler for: Dokumentationen er standardkontraktbestemmelser eller en afgørelse om tilstrækkeligt beskyttelsesniveau, understøttet af en vurdering af overførslens konsekvenser, som for en lille virksomhed kan være kort: berørte datakategorier, modtagerland, risiko, trufne supplerende foranstaltninger. Spørgsmål til leverandøren: På hvilket retsgrundlag overfører I data til tredjelande, og hvilke supplerende foranstaltninger anvender I?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

5.31 **De lovmæssige og aftalemæssige krav til behandlingen af personoplysninger er identificeret og holdes aktuelle, når retstilstanden ændrer sig. Modstridende jurisdiktioner er vurderet.**

Det taler for: Dokumentationen er en oversigt over de gældende krav (GDPR, nationale regler, branchespecifikke pligter) med en ansvarlig og en dato for gennemgang. I en lille virksomhed er en liste på en side, der gennemgås en gang om året, nok. Spørgsmål til leverandøren: Er I eller jeres underdatabehandlere underlagt jurisdiktioner, der giver myndigheder adgang til vores data, og hvordan håndterer I det?

◯ Åbent ◯ I gang ◯ Opfyldt ◯ Ikke relevant

Dokumentation / begrundelse

Kravene er formuleret selvstændigt og erstatter ikke standardens tekst. Kun originalstandarden fra den enkelte udgiver er bindende. Denne liste er et arbejdsredskab, ikke et bevis på overensstemmelse og ingen certificering. Leanshift er ikke certificeret efter nogen af disse standarder, er ikke et certificeringsorgan og har ingen forbindelse til ISO, IEC, DIN, IATF, IAQG eller SAE. I tvivlstilfælde gælder den tyske udgave af denne liste.