Bewaren, back-ups en beëindiging

ZorgPMO · 13 november 2026 · versie 2026-11-13.5

Beleidskader. Termijnen worden per klant vastgesteld en de uitvoering wordt aangetoond.

Uitgangspunt

Bewaar alleen wat noodzakelijk is voor een vastgelegd doel. Voor iedere gegevenscategorie registreert het omgevingsdossier termijn, eigenaar, verwijderwijze, uitzonderingen en bewijs. Archiveren is geen verwijderen. Dit document stelt geen automatische verwijdering van alle bestaande klantinhoud in werking.

Inhoud, accounts en exports

Tijdens actief gebruik beheert de klant de bewaartermijnen van projecten, documenten, notulen en opmerkingen. Bij beëindiging spreken partijen een export- en afwikkelperiode af. Het voorgestelde uitgangspunt is 30 dagen voor gecontroleerde teruggave, gevolgd door verwijdering uit actieve opslag. De klant bevestigt deze termijn voordat destructieve acties plaatsvinden.

Vertrekkende gebruikers verliezen hun toegang zodra de organisatie dat doorgeeft of zelf intrekt. Sessies, lidmaatschappen en tokens worden meegenomen. Historische bijdragen kunnen noodzakelijk blijven voor het projectdossier. Anonymisering of behoud wordt per doel beoordeeld. Exports en lokale kopieën bij de klant vallen onder diens beheer.

Logs en mail

Voor technische API-/securitylogs is 90 dagen een beleidsuitgangspunt. Verlenging voor een concreet incident vereist motivatie, beperkte toegang en een einddatum. Log geen volledige inhoud, tokens of wachtwoorden. Incidentdossiers en auditbewijs hebben een afzonderlijk vast te stellen termijn.

Verzonden technische mail in de platformwachtrij en de supportmailbox zijn verschillende gegevensbronnen. Voor de technische verzendadministratie is 90 dagen een uitgangspunt. Supportinhoud wordt op noodzaak beoordeeld en maximaal tot de afgesproken termijn na afhandeling bewaard. Maak expliciet afspraken met de mailprovider en over mailboxkopieën.

Back-ups en herstel

Leg back-upfrequentie en een eindige retentie vast. Een voorgesteld uitgangspunt voor reguliere herstelkopieën is 35 dagen, tenzij de klant een andere onderbouwde termijn afspreekt. Bestaande snapshots worden niet zonder gecontroleerd beleid en herstelbewijs verwijderd. De feitelijke configuratie moet overeenkomen met de bevestigde afspraak.

Back-ups zijn beperkt toegankelijk en worden niet voor normaal gebruik doorzocht. Bij herstel gelden eerdere verwijderverzoeken opnieuw. Uitzonderingen, bijvoorbeeld veiliggesteld incidentbewijs, krijgen een afzonderlijke eigenaar en einddatum. Een back-up zonder aantoonbaar bruikbare herstelroute vervult het continuïteitsdoel niet.

Offboardingcontrole

Controleer de bevoegdheid van het verzoek. Inventariseer inhoud, objectopslag, database, exports, logs, mail, tokens, koppelingen en back-ups. Leg de keuze voor teruggave of verwijdering vast. Plan uitvoering en eventueel een bezwaar-/correctietermijn.

Verifieer exportintegriteit, trek toegang in, verwijder uit actieve opslag en volg resterende kopieën tot het einde van hun retentie. Bewaar een verwijderbewijs met categorieën, datum, uitvoerder en gemotiveerde uitzonderingen, zonder de verwijderde inhoud daarin opnieuw op te nemen.

Actuele versie: https://zorgpmo.nl/vertrouwen/bewaarbeleid/