Dazr Compliance

Verwerkersovereenkomst

Laatst bijgewerkt op 7 oktober 2026 · Overeenkomst als bedoeld in art. 28 AVG.

Dit is een vertaling, alleen ter informatie. Bij verschillen tussen deze vertaling en de Engelse versie is de Engelse versie leidend.

Hoe dit werkt

Deze verwerkersovereenkomst maakt deel uit van de gebruiksvoorwaarden. Ze treedt automatisch in werking zodra een werkruimte wordt aangemaakt en daarin persoonsgegevens worden opgeslagen. De klantorganisatie die eigenaar is van de werkruimte is de verwerkingsverantwoordelijke; Dazr is de verwerker. Een handtekening is niet nodig; heeft je inkoopproces een door beide partijen ondertekend exemplaar nodig, mail dan naar legal@dazr.eu.

1. Definities

Begrippen in deze verwerkersovereenkomst hebben de betekenis die Verordening (EU) 2016/679 (de AVG) eraan geeft. "Persoonsgegevens van de klant" zijn persoonsgegevens die de verwerkingsverantwoordelijke (of de leden of auditors die onder haar verantwoordelijkheid handelen) in de werkruimte zet, waaronder persoonsgegevens in de inhoud van controletaken, bewijs, opmerkingen, bestanden, risico's, incidenten, leveranciersgegevens, leden en uitnodigingen, inzendingen via het openbare meldportaal en het activiteitenlogboek.

2. Onderwerp, duur, aard en doel

- Onderwerp: het verwerken van persoonsgegevens van de klant, zodat de verwerkingsverantwoordelijke haar complianceprogramma voor informatiebeveiliging en gegevensbescherming via het Dazr Compliance-platform kan beheren.
- Duur: de looptijd van het abonnement van de verwerkingsverantwoordelijke, plus de respijtperiode na beëindiging uit de gebruiksvoorwaarden.
- Aard en doel: hosting, opslag, verzending, opvraging, wissing en de handelingen die zijn beschreven in de gebruiksvoorwaarden en de privacyverklaring.
- Soort persoonsgegevens: identificatiegegevens van leden van werkruimtes en uitgenodigde auditors (e-mailadres, naam, rol); waar van toepassing identificatiegegevens van melders via het openbare meldportaal en van melders van incidenten; contactgegevens van werkgevers en operationele metadata die de verwerkingsverantwoordelijke uploadt. De verwerkingsverantwoordelijke is ervoor verantwoordelijk geen bijzondere categorieën van persoonsgegevens te uploaden, tenzij haar eigen grondslag dat toestaat.
- Categorieën van betrokkenen: werknemers, opdrachtnemers en uitgenodigde externe auditors van de verwerkingsverantwoordelijke, en alle personen die worden genoemd in compliance-inhoud die de verwerkingsverantwoordelijke besluit te uploaden.

3. Verplichtingen van de verwerker

1. We verwerken persoonsgegevens van de klant uitsluitend op basis van schriftelijke instructies van de verwerkingsverantwoordelijke. Die instructies bestaan uit het gebruik van de beoogde functies van het platform; zijn we van mening dat een instructie inbreuk maakt op de AVG of op ander Unierechtelijk of lidstatelijk recht inzake gegevensbescherming, dan stellen we de verwerkingsverantwoordelijke daarvan in kennis.
2. We zorgen ervoor dat de personen die gemachtigd zijn om persoonsgegevens van de klant te verwerken, zich tot geheimhouding hebben verbonden.
3. We nemen alle maatregelen die op grond van art. 32 AVG (beveiliging van de verwerking) vereist zijn. De huidige maatregelen staan in artikel 7 hieronder.

4. We leven de voorwaarden van art. 28 lid 2 en lid 4 na voor het inschakelen van subverwerkers (zie artikel 6).
5. Rekening houdend met de aard van de verwerking en de informatie waarover we beschikken, helpen we de verwerkingsverantwoordelijke bij het nakomen van haar verplichtingen om verzoeken van betrokkenen te beantwoorden, inbreuken te melden, DPIA's uit te voeren en voorafgaand overleg met toezichthoudende autoriteiten te voeren (art. 28 lid 3 sub e en f).
6. Na afloop van de dienstverlening wissen we, naar keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens van de klant of geven we die terug, en verwijderen we bestaande kopieën, tenzij opslag op grond van Unierecht of lidstatelijk recht verplicht is.
7. We stellen alle informatie ter beschikking die nodig is om de naleving van art. 28 aan te tonen, en maken audits, waaronder inspecties, mogelijk en dragen daaraan bij (zie artikel 9).

4. Verplichtingen van de verwerkingsverantwoordelijke

- De verwerkingsverantwoordelijke staat ervoor in dat zij een rechtmatige grondslag heeft op grond van art. 6 (en waar relevant art. 9) voor de persoonsgegevens die zij in de werkruimte zet.
- De verwerkingsverantwoordelijke is verantwoordelijk voor de juistheid van de persoonsgegevens van de klant en voor het beantwoorden van verzoeken van betrokkenen over haar werkruimte (verzoeken die wij ontvangen, sturen we aan de verwerkingsverantwoordelijke door, en we verlenen bijstand zoals vereist door art. 28 lid 3 sub e).
- De verwerkingsverantwoordelijke beheert de toegang - rollen van leden, uitnodigingen van auditors, het openbare meldportaal - via de instellingen van het platform.

5. Doorgifte naar derde landen

Persoonsgegevens van de klant worden opgeslagen en verwerkt op servers in de Europese Unie. Vercel, Upstash en Namecheap zijn bedrijven met zetel in de Verenigde Staten; mocht een van hen van buiten de EU toegang krijgen tot persoonsgegevens van de klant, dan valt die doorgifte onder de modelcontractbepalingen van de Europese Commissie (Besluit 2021/914), module 3 (verwerker aan verwerker), met de aanvullende maatregelen uit artikel 7. De actuele subverwerkers en hun serverregio’s staan op /legal/nl/subprocessors.

6. Subverwerkers

1. De verwerkingsverantwoordelijke geeft ons toestemming subverwerkers in te schakelen om de dienst te leveren. De huidige lijst staat op /legal/nl/subprocessors.
2. Wij informeren de verwerkingsverantwoordelijke ten minste 30 dagen vooraf over voorgenomen toevoegingen of vervangingen, per e-mail aan de eigenaar van de werkruimte en aan iedereen die ons via privacy@dazr.eu heeft gevraagd op de hoogte te worden gehouden.
3. De verwerkingsverantwoordelijke kan op redelijke gronden van gegevensbescherming bezwaar maken. Kunnen we niet aan het bezwaar tegemoetkomen, dan mag de verwerkingsverantwoordelijke de betreffende dienst beëindigen en ontvangt zij restitutie naar rato voor het ongebruikte deel van de lopende factuurperiode.
4. We leggen elke subverwerker bij schriftelijke overeenkomst verplichtingen inzake gegevensbescherming op die niet minder beschermend zijn dan die in deze verwerkersovereenkomst, en we blijven jegens de verwerkingsverantwoordelijke aansprakelijk voor het nakomen van de verplichtingen van de subverwerker.

7. Beveiligingsmaatregelen (art. 32)

- Versleuteling. Werkruimterecords worden door de applicatie met AES-256-GCM versleuteld voordat ze worden opgeslagen, bovenop de versleuteling in rust van de opslagprovider, met sleutels die (met HKDF-SHA-256) zijn afgeleid van een hoofdsleutel van 256 bits die alleen als geheim van de productieomgeving wordt bewaard, gescheiden van de opgeslagen data; de hoofdsleutel kan worden vervangen, waarna een achtergrondtaak de opgeslagen records opnieuw versleutelt. Geüploade bestanden

(bewijs, beleids- en profieldocumenten, bijlagen bij datalekmeldingen) worden in rust versleuteld door de opslagprovider, staan onder willekeurige, niet te raden adressen en worden alleen na een toegangscontrole geleverd; SBOM-bestanden in de module voor de Cyber Resilience Act worden ook door de applicatie versleuteld. Al het verkeer verloopt via HTTPS met HSTS preload; er is geen onversleuteld alternatief.

- Toegangsbeheer. Rolgebaseerd toegangsbeheer in het platform (eigenaar / beheerder / lid / auditor); tijdelijke en intrekbare auditorsessies. Operationele toegang is beperkt tot een klein supportteam via het supportportaal, dat bewust alleen metadata toont.
- Authenticatie. Inloggen zonder wachtwoord met Google of Microsoft (OpenID Connect) of een eenmalige code per e-mail; auditors bevestigen een eenmalige code per e-mail. Met HMAC ondertekende sessietokens met een beperkte geldigheid. Rate limiting op elk openbaar endpoint, ook de beheerderslogin.
- Veerkracht en integriteit. Een activiteitenlog van elke handeling die iets wijzigt, met de meest recente 2.000 tot 50.000 gebeurtenissen, afhankelijk van het abonnement. Back-ups binnen de EU. De integriteit van opgeslagen gegevens wordt gecontroleerd met AEAD-authenticatietags; gemanipuleerde versleutelde gegevens leveren een fout op en worden niet geserveerd.
- Netwerk en headers. Strikte Content-Security-Policy met een allowlist van gehashte inline scripts, strikte X-Frame-Options, X-Content-Type-Options nosniff en HSTS-preload.
- Kwetsbaarhedenbeheer. Afhankelijkheden zijn vastgepind; we volgen beveiligingsadviezen en installeren patches volgens een schema dat past bij de ernst.

8. Inbreuk in verband met persoonsgegevens

Als we kennis krijgen van een inbreuk in verband met persoonsgegevens die persoonsgegevens van de klant treft, informeren we de eigenaar van de werkruimte zonder onredelijke vertraging en uiterlijk binnen 72 uur nadat we er kennis van hebben gekregen (art. 33 lid 2). De melding beschrijft, voor zover bekend: de aard van de inbreuk, de waarschijnlijke gevolgen, de genomen of voorgestelde maatregelen en het contactpunt voor meer informatie. We helpen de verwerkingsverantwoordelijke bij haar eigen meldplichten op grond van art. 33 en art. 34.

9. Audits

De verwerkingsverantwoordelijke (of een door haar aangewezen externe auditor) mag eenmaal per twaalf maanden controleren of wij deze verwerkersovereenkomst naleven, met een schriftelijke aankondiging van ten minste 30 dagen en tijdens kantooruren, op een manier die onze bedrijfsvoering niet onredelijk verstoort en de vertrouwelijkheid van gegevens van andere klanten respecteert. Voor audits boven deze frequentie kunnen we een redelijke vergoeding vragen. Kan aan een auditverplichting op grond van art. 28 lid 3 sub h worden voldaan met een verklaring van een externe partij die wij hebben, dan verstrekken we die in plaats van een audit op locatie.

10. Aansprakelijkheid

De aansprakelijkheid van elke partij op grond van deze verwerkersovereenkomst is onderworpen aan de beperkingen in de gebruiksvoorwaarden. Die beperkingen gelden niet voor schade die betrokkenen lijden op grond van art. 82 AVG.

11. Duur en beëindiging

Deze verwerkersovereenkomst geldt zolang we persoonsgegevens van de klant verwerken, en blijft na beëindiging van de gebruiksvoorwaarden van kracht voor zover en zolang we nog zulke gegevens bewaren. De artikelen 8 (inbreuk), 9 (audits) en 12 (teruggave / verwijdering) blijven na beëindiging van kracht.

12. Teruggave en verwijdering

Bij beëindiging van de dienst kan de verwerkingsverantwoordelijke de gegevens van de werkruimte tijdens de respijtperiode van 30 dagen uit de gebruiksvoorwaarden exporteren met de exportfuncties van het platform. Na de respijtperiode verwijderen we de persoonsgegevens van de klant; back-ups verlopen volgens ons bewaarschema. Gegevens die we wettelijk moeten bewaren (bijvoorbeeld facturen op grond van het Italiaanse handelsrecht) bewaren we alleen zolang die verplichting geldt.

13. Rangorde

Bij strijdigheid tussen deze verwerkersovereenkomst en de gebruiksvoorwaarden of de privacyverklaring gaat deze verwerkersovereenkomst voor op het gebied van gegevensverwerking. Standaardcontractbepalingen die voor een doorgifte buiten de EU zijn opgenomen, gaan voor op zowel deze verwerkersovereenkomst als de gebruiksvoorwaarden voor de onderwerpen die zij regelen.

14. Kennisgevingen

- Aan Dazr: privacy@dazr.eu (gegevensbescherming) of security@dazr.eu (incidenten).
- Aan de verwerkingsverantwoordelijke: het e-mailadres van de eigenaar van de werkruimte dat op het moment van de kennisgeving bij ons bekend is.