

Beveiliging en privacybeheer

Voor Twilper.com en de handelsnamen Printen.eu en SendLetter. Eigenaar en aanspreekpunt: Gert Snijder, info@twilper.com. Er is geen formele Data Protection Officer aangesteld en de onderneming claimt geen eigen ISO 27001-, ISO 27701- of SOC 2-certificering.

Status en reikwijdte. Dit document legt de door de eigenaar gevraagde bedrijfsregels vanaf 22 oktober 2026 vast. Het is geen verklaring dat iedere maatregel al operationeel is of onafhankelijk is geaudit. De afzonderlijke uitvoeringscontrole blijft leidend voor antwoorden aan platforms. Bestaande privacyverklaringen en overeenkomsten blijven gelden; deze tekst vervangt geen verwerkersovereenkomst.

1. Verantwoordelijkheid en controle

Gert Snijder beheert het beleid, verleent toegang en beslist over incidenten en privacyverzoeken. Een ingeschakelde specialist krijgt alleen de toegang die voor een concrete taak nodig is. Minimaal jaarlijks en na een relevant incident of grote systeemwijziging worden beleid, toegangen, leveranciers en bewaartermijnen opnieuw beoordeeld. Elke beoordeling krijgt een datum, bevindingen en vervolgacties. Uitgevoerde controles worden geregistreerd; een beleidsregel alleen geldt niet als bewijs van uitvoering.

2. Gegevensclassificatie en doelbinding

Klasse	Voorbeelden	Behandeling
Openbaar	Productinformatie, openbare prijzen, algemene bestandsrichtlijnen	Mag via website en publieke productkoppelingen worden gedeeld.
Intern	Werkafspraken, interne technische documentatie en leveranciersvergelijkingen	Alleen voor medewerkers en bevoegde opdrachtnemers. Inkooprijzen worden niet in klantdocumenten gepubliceerd.
Vertrouwelijk	Klantcontact, aflevergegevens, ontwerpen, bijlagen, briefinhoud, gesprekken en orderinformatie	Alleen verwerken voor de gevraagde dienst, support, beveiliging en toepasselijke administratie. Geen gebruik voor ongevraagde marketing. Alleen delen met benodigde dienstverleners binnen hun overeengekomen rol.
Geheim	Wachtwoorden, tokens, API-sleutels en encryptiesleutels	Alleen in daarvoor bestemde beveiligde opslag. Geen sleutels in Git, klantmails, screenshots of logbestanden. Encryptiesleutels worden afzonderlijk beheerd van de versleutelde gegevens.

3. Toegangsbeheer

Toegang wordt per persoon of dienst verleend volgens minimale bevoegdheden. Beheer, klantfuncties en publieke koppelingen blijven gescheiden. Nieuwe of uitgebreidere toegang wordt door de eigenaar goedgekeurd. Beheerdersaccounts gebruiken multifactorauthenticatie waar de dienst dat ondersteunt. Toegangen worden ten minste per kwartaal en bij het einde van een samenwerking gecontroleerd en waar nodig ingetrokken. Tijdelijke accounts en testgegevens hebben een vast doel en worden niet stilzwijgend productieaccounts.

Productiegegevens worden niet naar onbeveiligde testomgevingen gekopieerd. Tests gebruiken synthetische gegevens of gecontroleerd geanonimiseerde kopieën. Toegang voor support wordt beperkt tot het probleem en geregistreerd waar de betreffende toepassing logging ondersteunt.

4. Technische basisregels

- Publieke diensten en gegevensoverdracht gebruiken HTTPS/TLS. Interne databaseverbindingen gebruiken een beveiligde verbinding passend bij de hostingdienst; de werkelijke instelling wordt per dienst gecontroleerd.
- Productieopslag en back-ups moeten passend versleuteld en afgeschermd zijn. Encryptie en toegangsinstellingen worden per gebruikte opslagdienst gecontroleerd; een certificering van een leverancier wordt niet als eigen certificering gepresenteerd.
- Werkstations met toegang tot klantgegevens moeten actuele beveiligingsupdates, malwarebescherming en automatische schermvergrendeling gebruiken. De uitvoering wordt per apparaat gecontroleerd.
- Geheimen worden alleen gedeeld met de dienst die ze nodig heeft. Rotatie gebeurt gecoördineerd met alle afhankelijke diensten; encryptiesleutels worden pas vervangen nadat bestaande gegevens veilig opnieuw kunnen worden ontsleuteld of versleuteld.
- Monitoring gebruikt zo weinig mogelijk persoonsgegevens. Complete bestanden, briefinhoud, tokens, wachtwoorden en sessiegeheimen horen niet in technische foutmeldingen. Bekende lekken in logging krijgen een afzonderlijke herstelactie en controle.
- Leveranciersaanvragen worden begrensd. Tests veroorzaken geen echte productie, betalingen, brieven of klantcommunicatie zonder de vereiste afzonderlijke toestemming.

5. Wijzigingen en kwetsbaarheden

Een foutmelding krijgt een reproduceerbare beschrijving, impact en eigenaar. De reparatie wordt los van ander onvoltooid werk uitgevoerd. Voor publicatie worden de relevante regressies en de vereiste buildcontroles uitgevoerd; daarna volgt een controle van de werkelijk gepubliceerde versie. Bewezen fouten krijgen voorrang op onbevestigde vermoedens. Beveiligingsupdates en meldingen van hosting- en softwareleveranciers worden beoordeeld op hun werkelijke impact. Een open controle of mislukte test wordt niet als voltooid aangemerkt.

6. Incidenten en datalekken

Een vermoeden wordt direct vastgelegd met ontdekkingstijd, betrokken systemen, feiten en nog onbevestigde punten. Gert Snijder leidt onderzoek en communicatie; een bevoegde specialist kan technisch onderzoek uitvoeren. Meldingen komen binnen via info@twilper.com. Systemen en toegangen worden waar nodig ingeperkt, bewijs wordt veiliggesteld en getroffen gegevens en betrokkenen worden beoordeeld.

Wanneer Twilper als verwerker optreedt, informeert het de verantwoordelijke klant en, waar van toepassing, het aangesloten platform zonder onredelijke vertraging overeenkomstig de geldende overeenkomst. Wanneer Twilper zelf verwerkingsverantwoordelijke is, beoordeelt het of melding aan de Autoriteit Persoonsgegevens en betrokkenen nodig is. Een verplichte melding aan de AP wordt binnen 72 uur na kennisname gedaan; zo nodig volgt aanvullende informatie later. Ook niet-meldingsplichtige inbreuken worden met de beoordeling geregistreerd. Na herstel volgen een oorzakonderzoek, controle en verbeteracties.

Bron voor het meldproces: Autoriteit Persoonsgegevens — zo meldt u een datalek. Een leveranciersstoring of algemeen beveiligingsbericht bewijst op zichzelf geen datalek bij Twilper.

7. Privacyverzoeken, bewaren en verwijderen

Verzoeken om inzage, correctie, overdracht, beperking of verwijdering worden via het gepubliceerde privacycontact behandeld. De identiteit en bevoegdheid worden passend gecontroleerd zonder meer gegevens te vragen dan nodig. Voor gegevens die namens een zakelijke klant worden verwerkt, wordt de verantwoordelijke klant betrokken. Verwijdering raakt de juiste gegevens en gekoppelde bestanden; een onafgeronde productieorder, wettelijke administratie en back-uprotatie worden afzonderlijk beoordeeld en uitgelegd.

Bewaartermijnen worden per dienst vastgelegd en sluiten aan op de gepubliceerde privacyverklaring, overeenkomst en werkelijke verwijderfunctie. Bij beëindiging van een koppeling wordt de toegang ingetrokken en worden tokens verwijderd of onbruikbaar gemaakt. Gegevens worden niet onbeperkt bewaard omdat een koppeling ooit actief was. Een automatische verwijderfunctie wordt pas ingeschakeld nadat scope, termijnen, uitzonderingen en gevolgen zijn gecontroleerd; een beleidsvoornemen is geen bewijs dat die taak al draait.

8. Hosting, verwerkers en AI

Per dienst wordt bijgehouden welke verwerkers en productiepartners nodig zijn, welke gegevens zij ontvangen en in welke landen opslag en verwerking plaatsvinden. Een EU-regio voor de database betekent niet automatisch dat alle leverancierondersteuning of alle verdere verwerking in de EU blijft. Er worden geen uitsluitend-EU-claims gedaan zonder bewijs voor de volledige keten. AI ontvangt alleen de informatie die nodig is voor de gevraagde functie. Een bestand wordt niet openbaar gemaakt om analyse mogelijk te maken; beeldherkenning wordt pas als werkend aangeboden wanneer de daadwerkelijke afbeelding veilig bij een geschikte verwerking terechtkomt.

9. Diensts specifieke informatie

De actuele privacyverklaringen zijn beschikbaar op Printen.eu en Twilper.com. SendLetter houdt een eigen verklaring voor briefverwerking en gekoppelde dienstverlening. Publieke productkoppelingen geven geen toegang tot mailboxen, beheerdersfuncties of willekeurige klantorders. Een orderstatus vraagt de daarvoor bedoelde controle; echte betaling of productie gebeurt in de daarvoor aangewezen gebruikersflow.

10. Bewijs en nog uit te voeren controles

Bij dit beleid hoort een uitvoeringsregister met per maatregel: systeem, eigenaar, bewijsdatum, resultaat en eventuele actie. Daarin worden onder meer apparaatbeveiliging, beheer-2FA, databaseverbindingen, opslag/back-ups, toegangscontrole, verwijderfunctie, verwerkers en incidentoefening afgetekend. Alleen daadwerkelijk gecontroleerde resultaten worden gebruikt voor externe beveiligingsvragenlijsten. Het bestaan van dit document mag niet worden gebruikt om onbekende of nog niet uitgevoerde maatregelen met "ja" te beantwoorden.