AVG-datalekmelding sjablonenpakket

Artikel 33-melding aan de autoriteit · Artikel 34-brief aan betrokkenen · Artikel 33(5)-datalekregister

GRATIS SJABLOON — DOCX · PDF · MD | Versie 1.0 · Bijgewerkt 2026-07-22

Document A — dien binnen 72 uur na kennisname in bij uw toezichthoudende autoriteit (AVG art. 33).

Document B — verstuur zonder onredelijke vertraging aan betrokkenen wanneer het risico hoog is (AVG art. 34).

Document C — leg elke inbreuk vast, gemeld of niet (AVG art. 33(5)).

Document D — de beslishulp melden-of-niet.

NL: meld bij de Autoriteit Persoonsgegevens via het meldloket datalekken. VK: meld bij de ICO. Noorwegen: bij Datatilsynet via Altinn.

Grensoverschrijdend in de EU/EER: meld bij uw leidende toezichthoudende autoriteit (art. 56).

Document A — Melding aan de toezichthoudende autoriteit (artikel 33)

Vul elke sectie in. De secties 2–5 sluiten aan op artikel 33(3)(a)–(d) — de wettelijke minimuminhoud. De 72-uursklok loopt vanaf kennisname (EDPB-richtsnoeren 9/2022): het moment waarop een verantwoordelijke persoon met redelijke zekerheid concludeert dat persoonsgegevens zijn gecompromitteerd.

A.1 Indieningsgegevens

Aan (toezichthoudende autoriteit)	Bevoegde autoriteit; leidende toezichthoudende autoriteit bij grensoverschrijdende verwerking (art. 56)
Van (verwerkingsverantwoordelijke)	Naam van de juridische entiteit en statutair adres
Incidentreferentie	Intern ID, bijv. BREACH-2026-007
Meldingstype	Initieel / Bijwerking / Definitief (gefaseerde melding, art. 33(4))
Ingediend (datum & tijd)	Tijdstip van deze indiening

A.2 Kennisname en tijdlijn (art. 33(1))

Tijdstip van kennisname	Wanneer een verantwoordelijke persoon concludeerde dat er waarschijnlijk een inbreuk was — start van de 72-uursklok
Hoe wij kennis kregen	Alert, verwerkersmelding onder art. 33(2), klantmelding, auditbevinding…
Redenen voor vertraging	VERPLICHT als deze indiening later is dan 72 uur na kennisname; anders n.v.t.

A.3 Aard van de inbreuk (art. 33(3)(a))

Wat er is gebeurd	Beschrijf het incident en de oorzaak; inbreuk op vertrouwelijkheid, integriteit en/of beschikbaarheid
Categorieën van betrokkenen	Bijv. klanten, medewerkers, eindgebruikers van klanten
Bij benadering aantal betrokkenen	Aantal of bereik; bijwerken in latere indieningen als het verandert
Categorieën van persoonsgegevens	Bijv. contactgegevens, inloggegevens, financiële gegevens — markeer bijzondere categorieën (art. 9) expliciet
Bij benadering aantal registers	Aantal of bereik

A.4 Contactpunt (art. 33(3)(b))

FG / contactpunt	Naam, rol, e-mail, telefoon — waar de autoriteit meer informatie kan verkrijgen

A.5 Waarschijnlijke gevolgen (art. 33(3)(c))

Waarschijnlijke gevolgen	Realistische schade: identiteitsfraude, oplichting, financieel verlies, reputatieschade, blootstelling van bijzondere categorieën

A.6 Genomen of voorgestelde maatregelen (art. 33(3)(d))

Indamming & herstel	Wat er is gedaan om de inbreuk aan te pakken
Beperking van nadelige gevolgen	Maatregelen die de schade voor betrokkenen verminderen, bijv. gedwongen wachtwoordreset, intrekking van inloggegevens

A.7 Standpunt over mededeling aan betrokkenen

Risicobeoordeling	Waarschijnlijk geen risico / risico / hoog risico — met korte redenering
Artikel 34-standpunt	Mededeling verzonden of gepland (datum), of uitzondering: 34(3)(a) onbegrijpelijke gegevens, 34(3)(b) risico weggenomen, 34(3)(c) openbare mededeling

A.8 Grensoverschrijdende verwerking (art. 56)

Grensoverschrijdend?	Zijn betrokkenen in meer dan één lidstaat geraakt?
Basis leidende autoriteit	Hoofdvestigingsredenering die de leidende toezichthoudende autoriteit aanwijst

Document B — Mededeling aan betrokkenen (artikel 34)

Vereist zonder onredelijke vertraging wanneer de inbreuk waarschijnlijk een HOOG risico oplevert. Duidelijke en eenvoudige taal; moet ten minste het contactpunt, de waarschijnlijke gevolgen en de maatregelen bevatten (art. 34(2) → art. 33(3)(b),(c),(d)). Vervang de tekst tussen haken; houd zinnen kort; vermijd jargon.

Onderwerp	Belangrijk beveiligingsbericht over uw persoonsgegevens
Wat er is gebeurd	[Eén of twee zinnen in eenvoudige taal: wat er gebeurde, wanneer het werd ontdekt en ingedamd.]
Welke gegevens het betreft	[De getroffen categorieën gegevens van de ontvanger. Benoem duidelijk wat NIET is geraakt, bijv. betaalgegevens.]
Wat dit voor u kan betekenen	[Realistische gevolgen — bijv. phishingmails die van ons afkomstig lijken, inlogpogingen.]
Wat wij doen	[Indamming, onderzoek, melding aan de toezichthoudende autoriteit, beveiligingsverbeteringen.]
Wat u kunt doen	[Concrete stappen: reset uw wachtwoord, schakel tweefactorauthenticatie in, let op verdachte e-mails, controleer afschriften.]
Waar u meer informatie vindt	[FG / contactpunt: naam, e-mail, telefoon — en een statuspagina indien beschikbaar.]
Afsluiting	Onze excuses voor de zorgen die dit incident kan veroorzaken. Wij houden u op de hoogte naarmate ons onderzoek vordert.

Variant openbare mededeling (art. 34(3)(c))

Zou het individueel benaderen van elke betrokkene onevenredige inspanning vergen, publiceer dan dezelfde inhoud als openbare mededeling (websitebanner, persbericht) die betrokkenen even doeltreffend informeert — en leg de kanaalkeuze en redenering vast in document C.

Document C — Interne registervermelding (artikel 33(5))

Vul één vermelding per incident in — ook voor inbreuken die u besluit NIET te melden. Via dit register toetst een toezichthoudende autoriteit de naleving van artikel 33.

Incidentreferentie	Intern ID
Tijdstip van kennisname / hoe	Wanneer de klok startte en wat de kennisname veroorzaakte
Feiten van de inbreuk	Aard, oorzaak, getroffen betrokkenen en registers
Gevolgen	Waargenomen werkelijke en waarschijnlijke gevolgen
Risicobeoordeling & redenering	Waarschijnlijk geen risico / risico / hoog risico — en waarom

Autoriteit geïnformeerd?	Ja (datum, referentie) / Nee — redenering: waarschijnlijk geen risico
Betrokkenen geïnformeerd?	Ja (datum, kanaal) / Nee — welke uitzondering van art. 34(3) en waarom
Verwerkersmelding (art. 33(2))	Welke verwerker ons informeerde en wanneer — als de inbreuk bij een verwerker ontstond
Herstelmaatregelen	Wat er als gevolg hiervan is hersteld, gewijzigd of verbeterd
Log van indieningen	Initiële / bijgewerkte / definitieve meldingen: datums en referenties

Document D — Beslishulp melden-of-niet

Situatie	Wat u moet produceren
Inbreuk levert waarschijnlijk geen risico op	Alleen document C — vastleggen met uw redenering
Inbreuk levert waarschijnlijk een risico op	Document A binnen 72u + document C
Inbreuk levert waarschijnlijk een HOOG risico op	Document A + document B zonder onredelijke vertraging + document C
Hoog risico, maar gegevens onbegrijpelijk (versleuteld, sleutels veilig) — art. 34(3)(a)	Document A + document C; geen document B
Hoog risico, maar latere maatregelen namen het weg — art. 34(3)(b)	Document A + document C; geen document B
Individuele brieven = onevenredige inspanning — art. 34(3)(c)	Document A + openbare mededeling + document C

De toezichthoudende autoriteit kan de mededeling aan betrokkenen bevelen op grond van art. 34(4), ook waar u concludeerde dat die niet vereist was. In Nederland accepteert de Autoriteit Persoonsgegevens een te late melding alleen in uitzonderlijke gevallen. Boetes voor schendingen van art. 33/34: tot 10 miljoen euro of 2% van de totale wereldwijde jaaromzet (art. 83(4)(a)).