| | |
|---|---|
| 32 761 | Verwerking en bescherming persoonsgegevens |
| 33 552 | Slachtofferbeleid |
| Nr. 343 | Brief van de staatssecretaris van Justitie en Veiligheid |

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 23 juni 2026

Uw Kamer heeft in de motie-Rajkowski c.s. de regering verzocht om te komen tot een duidelijk handelingskader voor slachtoffers van datalekken.[1] Daarnaast heeft uw Kamer in de motie-Kathmann/Dassen de regering verzocht om een wettelijke nazorgplicht te onderzoeken voor incidenten waarin op grote schaal persoonsgegevens worden gelekt, met als doel om de rechten van individuele slachtoffers en de plichten voor de getroffen instantie(s) in de wet vast te leggen, en dit onderzoek te betrekken bij de uitvoering van de eerdergenoemde motie-Rajkowski c.s.[2] Met deze brief informeer ik u, mede namens de staatssecretaris van Digitale Economie en Soevereiniteit, over de uitvoering van deze moties.

## Inleiding

Bescherming van persoonsgegevens vereist een adequaat beveiligingsniveau. Daarmee kunnen inbreuken in verband met persoonsgegevens (kortweg: datalekken) worden voorkomen, en ook de gevolgen daarvan.[3] Wat die gevolgen zijn, verschilt van

---

[1] *Kamerstukken II* 2025/26, 36 800-VII, nr. 78 (Motie van het lid Rajkowski c.s.). Deze motie is ingediend bij het Wetgevingsoverleg commissie Digitale Zaken, ter behandeling van de ontwerpbegrotingen BZK, EZ en JenV , voor zover het onderwerpen betreft die zien op digitale zaken, op 2 maart 2026 (Kamerstuk 36800 VII, nr. 96).

[2] *Kamerstukken II* 2025/26, 36 764, nr. 27 (Gewijzigde motie van de leden Kathmann en Dassen). Deze motie is ingediend bij het Wetgevingsoverleg Wet weerbaarheid kritieke entiteiten (36765) en Cyberbeveiligingswet (36764), op 23 maart 2026 (Kamerstuk 36764, nr. 32).

[3] De verwerking van persoonsgegevens moet voldoen aan de belangrijke beginselen van artikel 5 Algemene verordening gegevensbescherming (hierna: AVG). De bevoegd toezichthouder, de Autoriteit persoonsgegevens, heeft uw Kamer in een technische briefing op 13 mei 2026 over dit onderwerp nader geïnformeerd. Artikel 5, eerste lid, onder f AVG stelt: [Persoonsgegevens moeten] “door het nemen van passende

geval tot geval. Voor iedereen geldt dat de vertrouwelijkheid van aan een organisatie toevertrouwde persoonsgegevens is geschonden. Sommige mensen merken na een datalek geen, of niet meteen, gevolgen. Voor anderen zijn de gevolgen wel merkbaar, en soms heel ernstig. Hoewel elk datalek er één te veel is, brengen niet alle meldingen de hoogste risico's voor de door het datalek getroffen personen met zich mee. Zo valt het per ongeluk verwijderen van klantgegevens ook onder het begrip datalek. Tegelijkertijd kan één datalek ook betrekking hebben op een groot aantal mensen. Bij meer dan 5000 door een datalek getroffen personen dat waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van personen wordt gesproken van een groot datalek. Deze brief heeft op die categorie betrekking.  Het uitgangspunt van dit kabinet is dat datalekken waar mogelijk voorkomen dienen te worden. In deze brief zal ik daarom in de eerste plaats ingaan op de noodzaak van een adequaat beveiligingsniveau.

Helaas zijn er in de praktijk geregeld datalekken, en dus ook mensen die door een datalek worden getroffen. Zij zijn van het datalek slachtoffer. Daarbij neemt het aantal datadiefstallen toe.[4] Bij elk datalek, ook bij grote datalekken, is het van belang dat de gevolgen voor hen zo beperkt mogelijk zijn. Organisaties hebben op grond van de Algemene verordening gegevensbescherming (AVG) verplichtingen, die in dat kader een preventieve werking hebben. Ook in reactie op een groot datalek zijn organisaties tot acties verplicht. De organisatie dient slachtoffers in duidelijke en eenvoudige taal over een groot datalek te informeren. Deze

---

technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging". Artikel 32 AVG geeft nadere regels m.b.t. de beveiliging van de verwerking.

[4] De Autoriteit Persoonsgegevens (AP) rapporteerde in haar meest recente datalekkenrapportage dat er in 2024 37.839 datalekken bij haar werden gemeld. Een melding is op grond van artikel 33, eerste lid, AVG verplicht, indien er een risico is voor de rechten en vrijheden van natuurlijke personen. De Autoriteit Persoonsgegevens beoordeelt het risico op schade dat slachtoffers van een datalek lopen. In 2024 is naar 28 meldingen onderzoek gedaan. Op 11.024 meldingen is verdiepend toezicht gehouden. Hierbij ziet de AP grote risico's voor slachtoffers. De overige 26.815 datalekken zijn gemonitord. Zie Rapportage datalekken 2024 | Autoriteit Persoonsgegevens.

informatievoorziening aan slachtoffers is een belangrijk onderdeel van de opvolging die organisaties moeten geven aan een groot datalek. Hieraan besteed ik in deze brief in de tweede plaats aandacht.

Na een groot datalek kunnen slachtoffers vragen of zorgen hebben. Die vragen en zorgen zijn begrijpelijk en terecht. Duidelijke informatie voor slachtoffers is van wezenlijk belang om de risico's te beheersen. Om uitvoering te geven aan de motie-Rajkowski c.s. en de motie-Kathmann/Dassen, en om een beter beeld over de behoeften van slachtoffers te krijgen, is onderzoek uitgezet via de online research community 'Nederland denkt mee'. Daarnaast is een brede kennistafel met experts georganiseerd. Aan deze kennistafel namen verschillende instanties deel, waaronder toezichthouders. Op basis van het onderzoek en de informatie die is gewisseld tijdens de kennistafel constateer ik dat er aanleiding bestaat om in de eerste plaats organisaties ertoe aan te zetten slachtoffers beter te informeren over hoe zij risico's kunnen beheersen, en in de tweede plaats om als overheid duidelijke informatie hieromtrent ter beschikking te stellen. Deze twee acties vat ik samen onder de term 'duidelijk handelingskader slachtoffers grote datalekken'. Hierbij zal in deze brief daarom in de derde plaats worden stilgestaan.

**Noodzaak van een adequaat beveiligingsniveau**

Persoonsgegevens die aan een organisatie zijn toevertrouwd, dienen adequaat te worden beveiligd. Zo blijven persoonsgegevens beschermd, tegen interne fouten, zoals ongeautoriseerde wijziging van gegevens, maar ook tegen externe acties, zoals datadiefstallen. De impact op degenen van wie persoonsgegevens zijn buitgemaakt kan heel groot zijn. Bij online oplichting bijvoorbeeld, raken zij niet alleen hun geld kwijt, maar soms ook het vertrouwen om digitaal hun zaken te regelen. Daarnaast bestaat er bij veel slachtoffers van online oplichting een schuld- en schaamtegevoel. De aangiftecijfers liggen laag. Uit de recente Veiligheidsmonitor van het Centraal Bureau voor de Statistiek (CBS) blijkt dat 17% van de Nederlandse bevolking van 15 jaar en ouder in 2025 slachtoffer is geworden van een of meer online delicten of

incidenten.[5] Dit betreft vormen van digitale criminaliteit, variërend van phishing en hacken tot online oplichting en fraude. Ten opzichte van 2023 is ook het slachtofferschap van online criminaliteit licht gestegen, wat duidt op een toename en gestegen impact ervan op de samenleving. Deze cijfers ondersteunen de noodzaak van een adequaat beveiligingsniveau, om slachtoffers te voorkomen.

Dat is niet vanzelfsprekend een gemakkelijke opgave. Zoals het Cybersecuritybeeld Nederland 2025 laat zien wordt het digitale dreigingslandschap steeds meer divers en onvoorspelbaarder.[6] Criminele, statelijke én staatsgesteunde actoren begeven zich op het digitale strijdtoneel, ontwikkelen cybercapaciteiten en zetten deze in. Verder kunnen kwaadwillenden generatieve AI inzetten, waardoor zij aanvallen eenvoudiger en op grotere schaal kunnen uitvoeren. Al deze ontwikkelingen vinden gelijktijdig en in samenhang met elkaar plaats, waardoor het dreigingslandschap in toenemende mate complex wordt.[7] Voor allerlei typen actoren kunnen persoonsgegevens interessant zijn. De gegevens kunnen worden gestolen en doorverkocht, of ze kunnen worden gebruikt (als opstap) voor een toekomstige aanval.

De AVG vereist dat organisaties passende technische en organisatorische maatregelen nemen, om persoonsgegevens te beveiligen. Organisaties kunnen voor het identificeren van de risico’s ook gebruik maken van bijvoorbeeld de informatie van het Nationaal Cyber Security Centrum (NCSC). Met de Nederlandse Cybersecurity Strategie 2022-2028 zet het kabinet in op het verkleinen van de scheefgroei tussen de digitale dreiging en de weerbaarheid. Een belangrijk onderdeel daarvan is de implementatie van de Cyberbeveiligingswet (Cbw). Vanaf het moment van inwerkingtreding van de Cbw, waarin de Europese NIS2-richtlijn wordt geïmplementeerd, gelden op grond van die wet verplichtingen voor de in die wet genoemde organisaties met

---

[5] Veiligheidsmonitor 2025, CBS
[6] Cyber Security Beeld Nederland (CSBN) 2025, NCTV, 26-11-2025, https://www.nctv.nl/documenten/2025/11/26/cybersecuritybeeld-nederland-2025
[7] Cyber Security Beeld Nederland (CSBN) 2025, NCTV, 26-11-2025, https://www.nctv.nl/documenten/2025/11/26/cybersecuritybeeld-nederland-2025, p.5

betrekking tot de beveiliging van hun netwerk- en informatiesystemen. Onderdeel van deze wet zal een zorgplicht zijn die inhoudt dat organisaties die onder de wet vallen verplicht zijn tot het nemen van passende en evenredige, technische, operationele en organisatorische maatregelen, om de risico's met betrekking tot de beveiliging van hun netwerk- en informatiesystemen te beheersen. Ook moeten zij die maatregelen nemen om incidenten, waarbij bijvoorbeeld de beschikbaarheid of vertrouwelijkheid van systemen of van de daarin verwerkte gegevens in gevaar komt, te voorkomen en om de gevolgen daarvan te beperken. Ook geldt voor hen de verplichting om significante incidenten, indien die zich toch voordoen, te melden bij hun bevoegde autoriteit en hun *Computer security incident response team* (CSIRT), zodat op basis daarvan onder meer door het CSIRT bijstand kan worden verleend bij het treffen van maatregelen om de continuïteit van hun dienstverlening te herstellen. Bij dergelijke incidenten kan het ook gaan om incidenten waarbij persoonsgegevens in het geding zijn, maar daarvan hoeft niet noodzakelijkerwijs sprake te zijn. De Cbw regelt ook dat op de naleving van deze verplichtingen toezicht wordt gehouden.

Zoals eerder al benoemd is een adequaat beveiligingsniveau ook op grond van de AVG vereist om bescherming van persoonsgegevens te waarborgen en datalekken te voorkomen. De bevoegd toezichthouder, de Autoriteit Persoonsgegevens (AP), constateert dat het beveiligingsniveau van bedrijven en organisaties over het algemeen zowel technisch als organisatorisch te laag ligt.[8] De AP acht het onder meer van groot belang dat organisaties goed inzicht krijgen in risico's en te nemen maatregelen, en kritisch nadenken over het verwerken en bewaren van gegevens. In dat kader werd recent aangekondigd dat de AP preventief ICT-leveranciers gaat controleren op hun digitale beveiliging. Daarnaast houdt de Rijksinspectie Digitale Infrastructuur (RDI) ook toezicht op de digitale weerbaarheid van de sector digitale infrastructuur. Dit draagt bij aan de veiligheid van de producten en diensten die organisaties van deze ICT-leveranciers afnemen.

[8] Position paper AP t.b.v. rondetafelgesprek Cyberveiligheid en informatiebeveiliging d.d. 20 mei 2026, nr.2026D21931: https://www.tweedekamer.nl/downloads/document?id=2026D21931

## Noodzaak van beperking van de gevolgen en informatievoorziening

Mensen hebben veel belang bij het voorkomen van datalekken. Op die manier blijven hun in vertrouwen overhandigde persoonsgegevens beschermd. Daarnaast dienen er zo min mogelijk gegevens buit te kunnen worden gemaakt om de gevolgen van een datalek zo beperkt mogelijk te houden. In de inleiding werd al beschreven dat organisaties op grond van de AVG verplichtingen hebben, die daaraan bijdragen. Zoals het bij verwerking van persoonsgegevens naleven van de beginselen van artikel 5 AVG, waaronder dataminimalisatie en bewaartermijnen. Dit houdt in dat organisaties zo min mogelijk gegevens van betrokkenen verwerken, en deze gegevens niet langer bewaren dan noodzakelijk. Voor een digitaal toegangskaartje voor een eenmalig event is bijvoorbeeld niet nodig om het huisadres van de koper op te slaan, en ook niet om de personalia van de koper nog jaren te bewaren. Dataminimalisatie en de naleving van bewaartermijnen dragen eraan bij om de gevolgen van grote datalekken voor slachtoffers zo beperkt mogelijk te houden. De AVG bevat ook verplichtingen voor organisaties over het informeren van de Autoriteit Persoonsgegevens en over het informeren van de slachtoffers bij een groot datalek. Op grond van artikel 33 van de AVG meldt een organisatie een datalek, dat waarschijnlijk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, zonder onredelijke vertraging bij de AP. Op grond van artikel 34 van de AVG dient de organisatie onverwijld de slachtoffers te informeren dat er een datalek heeft plaatsgevonden, indien dit datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van personen. Daarbij moet in duidelijke en eenvoudige taal het datalek worden omschreven, de waarschijnlijke gevolgen, en de maatregelen die door de organisatie worden genomen om het datalek aan te pakken en de nadelige gevolgen ervan te beperken. De verplichte melding bij de AP en de verplichting om slachtoffers te informeren, opdat zij de risico’s die uit het datalek volgen kunnen beheersen, is een belangrijk onderdeel van de opvolging die organisaties moeten geven aan een groot datalek. Hieruit volgt dat plichten voor organisaties op het gebied van een datalek, en daarmee samenhangende rechten van degenen wiens persoonsgegevens bij het datalek betrokken zijn, al in de AVG zijn opgenomen. Organisaties dienen deze wettelijke verplichtingen na

te leven. De AP houdt hierop toezicht. Daarmee ziet het kabinet geen noodzaak voor een additionele wettelijke nazorgplicht.

## Handelingskader slachtoffers van grote datalekken

Om uitvoering te geven aan de motie-Rajkowski c.s. en de motie-Kathmann/Dassen zijn een aantal acties ondernomen. In de eerste plaats is onderzoek uitgezet via de online research community ‘Nederland denkt mee’. In de tweede plaats is een brede kennistafel met experts van verschillende instanties georganiseerd.

### *Onderzoek via online research community ‘Nederland denkt mee’*

Om een beter beeld te krijgen van ervaringen, behoeften, vragen, zorgen en verwachtingen van (potentiële) slachtoffers van een groot datalek, is kwalitatief onderzoek uitgevoerd in de online research community ‘Nederland denkt mee’.[9] Het onderzoek onderschrijft dat veel mensen ervaring hebben met grote datalekken. Vooral naam- en contactgegevens zijn daarbij gelekt, voor zover bij hen bekend. Een groot datalek heeft behoorlijke impact op slachtoffers, zo geven zij aan. Door het grote datalek voelen zij zich onzeker, onveilig, en ervaren zij verlies van controle. Deze impact wordt versterkt doordat slachtoffers in de periode na het grote datalek regelmatig worden lastiggevallen met spam, phishingmails, en verdachte telefoontjes. Slachtoffers hebben behoefte aan duidelijkheid, zekerheid en concrete handelingsperspectieven. Zij verwachten dat de organisatie waar het grote datalek heeft plaatsgevonden, de verantwoordelijkheid neemt en hen direct en op de persoon toegesneden wijze informeert en ondersteunt bij het nemen van actie. Ook verwachten zij dat, indien relevant, zij op de hoogte worden gehouden van ontwikkelingen. Het onderzoek stelt dat organisaties momenteel tekortschieten in het verstrekken van duidelijke informatie. Dat maakt ook dat slachtoffers zelf op zoek gaan naar aanvullende informatie. Daarbij raadplegen zij onder meer informatie van overheidsinstanties, maar ook bronnen op social media. Kort samengevat willen slachtoffers na een groot datalek begrijpen wat er is gebeurd, welke gegevens zijn gelekt, wat de mogelijke

[9] Het onderzoeksrapport is als bijlage bij deze brief gevoegd.

gevolgen zijn, en wat zij zelf kunnen doen aan maatregelen om risico's te beperken. Waar nodig verwachten zij geïnformeerd te blijven worden.

*Brede kennistafel met experts van verschillende organisaties*

Door ambtenaren van onze ministeries is een kennistafel georganiseerd om maatregelen te bespreken die voor slachtoffers van grote datalekken zijn en kunnen worden genomen. Aan deze kennistafel namen experts van verschillende instanties deel, zoals de AP, de RDI, het ECP – Platform voor de Informatiesamenleving, de Consumentenbond, de politie, de Fraudehelpdesk, het Centrum voor Criminaliteitspreventie en Veiligheid, de Rijksdienst voor Identiteitsgegevens, het Centraal Meldpunt Identiteitsfraude, en een onderzoeker. Veel van de aanwezigen meldden dat hun instantie na recente grote datalekken veel (extra) telefoontjes heeft ontvangen van slachtoffers. Voor slachtoffers wordt op de websites van deze instanties informatie en advies geboden. Denk aan het stappenplan dat de AP biedt,[10] maar bijvoorbeeld ook aan 'Check je hack' van de politie.[11] Op basis van het besprokene maak ik op dat ook de experts van mening zijn dat het van groot belang is dat organisaties de aan hen toevertrouwde persoonsgegevens adequaat beschermen. Daarnaast achten experts het belangrijk dat deze organisaties na een eventueel groot datalek voldoende en goede informatie aan slachtoffers verstrekken. Zij signaleren daarbij dat goede informatievoorziening voorkomt dat slachtoffers zelf op zoek gaan naar (aanvullend) advies, en daarmee mogelijk ook door desinformatie op social media worden beïnvloed. Daarbij is het ook relevant dat organisaties meer transparantie bieden over de persoonsgegevens die zij verwerken, bijvoorbeeld met een duidelijke pagina op de website. Tot slot moet duidelijke, betrouwbare informatie ook goed vindbaar zijn.

*Naar een duidelijk handelingskader voor slachtoffers van grote datalekken*

Op basis van het onderzoek via de online research community en de kennistafel met experts kom ik tot de volgende contouren voor

[10] Slachtoffer van een datalek? Dit kunt u doen | Autoriteit Persoonsgegevens
[11] Check je hack | politie.nl

een duidelijk handelingskader voor slachtoffers van grote datalekken.

Een organisatie moet na een groot datalek de slachtoffers zo snel mogelijk voorzien van duidelijke en betrouwbare informatie, waar mogelijk op de persoon toegesneden. Zij hebben het recht te weten wat er is gebeurd, welke gegevens zijn gelekt, wat de mogelijke gevolgen zijn, en wat zij zelf kunnen doen aan maatregelen om risico's te beperken. Die informatie dient zo spoedig mogelijk na het ontdekken van een groot datalek aan slachtoffers te worden verstrekt, maar ook in de periode daarna, voor zolang en zover dat relevant is. Indien aangewezen kan ook het informeren over compensatie daarvan onderdeel uitmaken.

Het kabinet vindt het van belang dat door een groot datalek getroffen organisaties deze informatie actief aan slachtoffers verstrekken. Hierbij wordt opgenomen welke informatie slachtoffers in ieder geval moeten ontvangen, welke voorbeeldteksten daarvoor kunnen worden gebruikt, en wat het handelingsperspectief is bij uiteenlopende risicoprofielen. Dat betreft bijvoorbeeld categorieën slachtoffers voor wie het bekend worden van persoonsgegevens bijzondere risico's met zich meebrengt. Hierin kan ook aandacht worden besteed aan meer informatie op maat voor kwetsbare groepen, bijvoorbeeld via seniorencafés of contact via professionals en zorgverleners. Ook dient informatie te worden verstrekt over de acties die door een groot datalek getroffen organisaties zelf hebben ondernomen, en welke verbeteringsmaatregelen zij zullen doorvoeren. Van belang is daarnaast duidelijkheid te bieden over welke maatregelen slachtoffers na een groot datalek kunnen nemen, en welke stappen zij daartoe kunnen zetten. Dit bevat in ieder geval informatie over welke beveiligingsmaatregelen iemand kan nemen. Denk aan het controleren of persoonsgegevens gelekt zijn, het wijzigen van wachtwoorden, de meerwaarde van het vervangen van eventuele identiteitsdocumenten, en het installeren van twee factor authenticatie. Tot slot dient aandacht te bestaan voor de consequenties als risico's niet tijdig beheerst kunnen worden. Denk aan financieel herstel (zoals hulp bij bankfraude), identiteitsherstel, en psychosociale ondersteuning. Verschillende slachtoffers hebben immers mogelijk verschillende behoeftes.

**Conclusie**

Het streven is erop gericht dat dat het handelingskader op korte termijn wordt afgerond, in overleg met relevante instanties, betrokken toezichthouders en vertegenwoordigers van het bedrijfsleven. Deze informatie kan vervolgens door de AP, als onderdeel of naar aanleiding van de meldingsprocedure voor datalekken, aan organisaties worden aangeboden, en op de websites van de betrokken instanties ter beschikking worden gesteld. Uw Kamer zal nog dit jaar nader worden geïnformeerd.

Met hetgeen hiervoor is geschetst wordt uitvoering gegeven aan de motie-Rajkowski c.s. om te komen tot een handelingskader voor slachtoffers van datalekken. Daarnaast is uitvoering gegeven aan de motie-Kathmann/Dassen. Ik constateer dat het recht van slachtoffers om goed te worden geïnformeerd, en de plicht van organisaties om slachtoffers na een datalek goed te informeren, reeds in de AVG zijn vastgelegd. De noodzaak van een adequaat beveiligingsniveau volgt daarnaast uit zowel de AVG als, voor zover relevant, de Cyberbeveiligingswet. Daarmee ziet het kabinet geen noodzaak voor een additionele wettelijke nazorgplicht voor incidenten waarin op grote schaal persoonsgegevens worden gelekt, zoals in de motie-Kathmann/Dassen is voorgesteld.

Dit neemt niet weg dat er verbeteringen mogelijk zijn. Met deze inzet beoogt het kabinet de bescherming van slachtoffers bij grote datalekken verder te versterken, de informatievoorziening te verbeteren en de naleving door organisaties te verbeteren. Wij houden uw Kamer van de voortgang op de hoogte.

De staatssecretaris van Justitie en Veiligheid,
K.T. van Bruggen