

 @zWenne

Meldplicht datalekken

Prof. mr. G-J. (Gerrit-Jan) ZWENNE | Leiden

2 februari 2016



Universiteit
Leiden



programma

A. update

stand van zaken met betrekking tot dé verordening

wat is er gebeurd op 1 januari jl?

B. meldplicht datalekken

C. bestuurlijke boetebevoegdheid



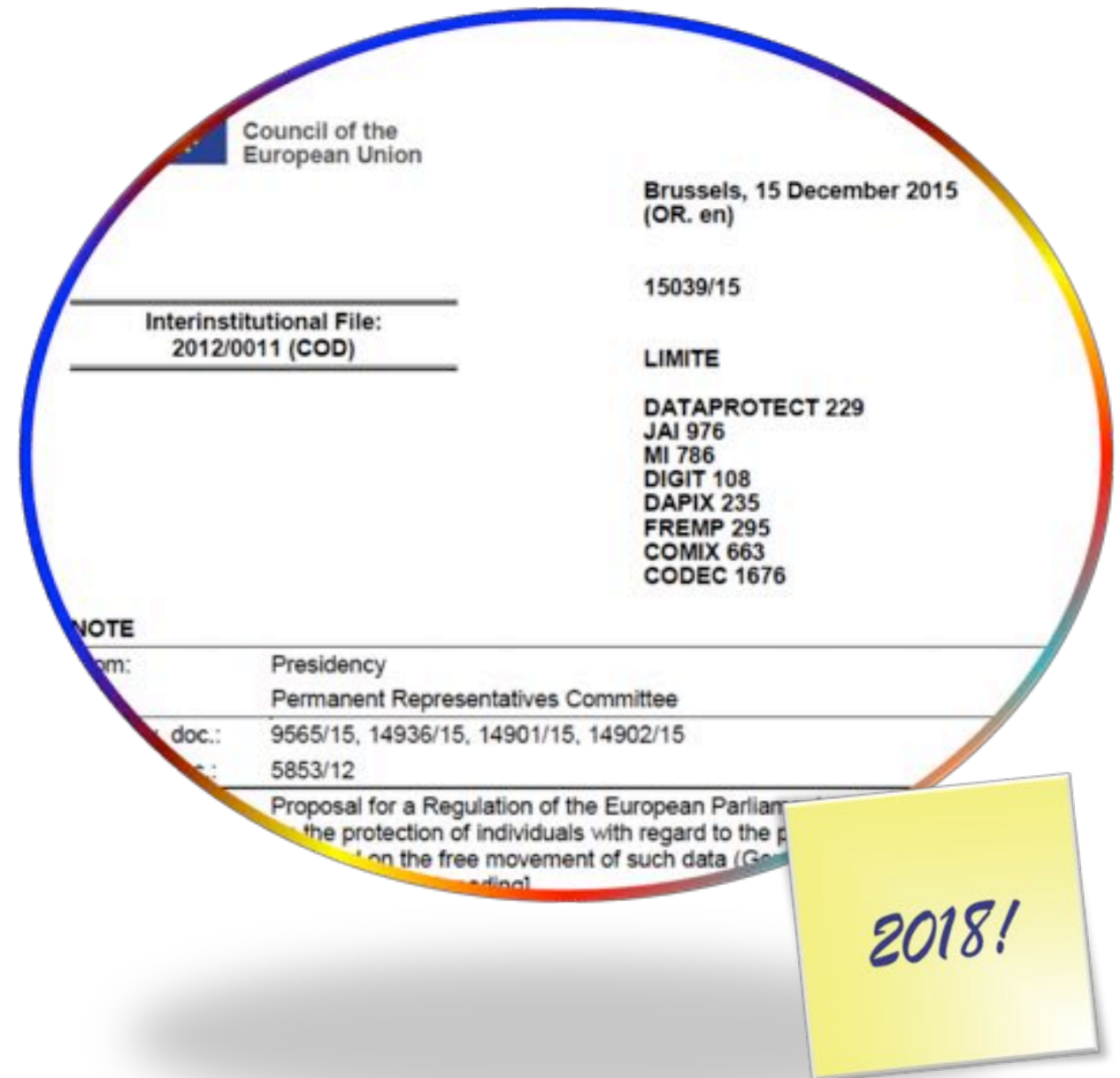
A. UPDATE

algemene verordening gegevensbescherming

Proposal for a General Data Protection Regulation of 15 December 2015:
'overall compromise tekst'

veel meer van alles:

- veel grotere reikwijdte, breder toepassingsbereik
- meer verplichtingen voor verantwoordelijken én voor bewerkers (incl. **meldplicht**)
- meer rechten voor betrokkenen (datasubjects)
- meer formaliteiten
- meer bevoegdheden voor toezichthouders en veel hogere boetes



Vanaf 1 januari 2016

Stb. 2015, 230

- Meldplicht datalekken
- Uitbreiding bestuurlijke boetebevoegdheid Cbp

Hoofdstuk 9. Toezicht
Paragraaf 1. Het College bescherming
persoonsgegevens

Artikel 51

1. Er is een College bescherming persoonsgegevens dat tot taak

4. Het College wordt in het maatschappelijk verkeer aangeduid als: Autoriteit persoonsgegevens





bestuurlijke boetes

vanaf 1 januari 2016

max. €20.250

art. 4(3)a, 78(2) a Wbp

max. €450.000

art. 11.3a Tw en 5:20(1) Awb

max. €820.000

art. 6-9(1), 9(4), 11-13, 16, 24, 33-36, 38-42, 66,
76-78 Wbp en 5:20(1) Awb

10 procent jaaromzet
indien passend...

wellicht vanaf 1 mei 2018

€10.000.000 of €20.000.000 danwel
2 of 4 procent van wereldwijde
groepsomzet (*“whichever is greater”*)



B. MELDPLICHT DATALEKKEN

Meldplicht datalekken

Melding bij toezichthouder

bij 'aanzienlijke kans op ernstige nadelige gevolgen of ernstige nadelige gevolgen voor de bescherming van persoonsgegevens'

Melding bij betrokkene

bij 'waarschijnlijk ongunstige gevolgen voor diens persoonlijke levenssfeer'



Wie?

verantwoordelijke

Wat?

inbreuk op beveiliging van persoonsgegevens

Wanneer?

onverwijld d.w.z. in beginsel binnen 72 uur na bekend worden van het datalek

Hoe?

Meldloket Datalekken (Ap)

zo-mogelijk individueel (betrokkenen)

‘inbreuk op beveiliging van persoonsgegevens’

gegevens betreffende geïdentificeerde of identificeerbare natuurlijke personen

Wél: werknemers, ambtenaren, studenten, scholieren, zzp-ers, contactpersonen, patiënten, consumenten, kinderen, volwassenen, leden, treinreizigers, automobilisten, etc.

Niet: rechtspersonen, bedrijven, overledenen

- *passende technische en organisatorische maatregelen om persoonsgegevens te **beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.***
- *maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.*
- *maatregelen moeten onnodige verzameling en verdere verwerking van persoonsgegevens voorkomen*

beveiligingsmaatregelen

preventieve maatregelen

- voorkomen dat een dreiging leidt tot een incident

detectieve maatregelen

- vaststellen dat er een incident is geweest

repressieve maatregelen

- beperken van negatieve gevolgen van het incident

herstelmaatregelen

- herstel van negatieve gevolgen



correctieve maatregelen

- reparatie van tekortkomingen in de beveiliging

inbreuk

er is niet uitsluitend sprake van een dreiging of een tekortkoming in de beveiliging maar er heeft zich **daadwerkelijk een beveiligingsincident** voorgedaan

de preventieve maatregelen waren niet toereikend om dit te voorkomen.

er zijn **daadwerkelijk gevolgen** voor de verwerkte persoonsgegevens:

- er zijn persoonsgegevens verloren gegaan
- niet uit te sluiten dat er gegevens onrechtmatig zijn verwerkt

de getroffen repressieve maatregelen en de herstelmaatregelen waren onvoldoende om negatieve gevolgen geheel weg te nemen

verloren USB-stick

gestolen laptop

sql-hack *malware*

ransomware

brand in datacentrum



gebruikersnaam en wachtwoord

Een werknemer geeft een kennis haar gebruikersnaam en wachtwoord die toegang geven tot de klantgegevens van het bedrijf waar zij werkt.

Dit wordt ontdekt. Het bedrijf past het wachtwoord aan. Daarmee heeft de kennis geen toegang meer.

Aan de hand van logbestanden gaat het bedrijf na of de derde daadwerkelijk toegang heeft gehad tot de klantgegevens.

Er kan redelijkerwijs worden uitgesloten dat er door middel van het betreffende account toegang is verkregen tot de gegevens.

Melding..?

accounts passwords hack

op pastebin.com wordt een lijst gepubliceerd met 16,5 miljoen wachtwoorden van een populair sociaal netwerk

Melding..?



Melding bij Ap

Melding bij toezichthouder

(aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens



- *bijzondere gegevens (art. 16)*
- *financiële of economische gegevens*
- *stigmatiserings- c.q. uitsluitingsrisico's*
- *gebruikersnamen, wachtwoorden, identiteitsfraude e.d.*
- *beroepsgeheim, DNA-gegevens*

- *omvang van lek (aantal personen en/of hoeveelheid gegevens)*
- *ingrijpendheid van o.b.v. gegevens genomen beslissingen*
- *olievlek (bijv. ketensamenwerking)*

Wél melden

- technische storing in ziekenhuis waardoor medische gegevens zijn ingezien door onbevoegden
- kopieën paspoort of rijbewijs, bank- of creditcardnrs, wachtwoorden, enz.
- laptop met onversleutelde financiële gegevens
- tablet met versleutelde gegevens, maar geen back-up
- envelop met creditcardgegevens

Níet melden

- foutief geadresseerde brief, ongeopend teruggestuurd
- zoekgeraakte en ongeopend teruggevonden koffer
- verloren ledenadministratie van tennisvereniging
- ziekenhuispersoneel 'leent' wachtwoord van co-assistent

*bestand i.d.z.v.
art. 1(c) Wbp...?*

'onverwijld'

vanaf moment van bekend worden van datalek

- door verantwoordelijke zelf
- door bewerker(!)

zonder onnodige vertraging

- zo mogelijk niet later dan 72 uur na ontdekking
- maar later mag als dat kan worden uitgelegd

idem art. 31(1) GDPR



melding aan betrokkene

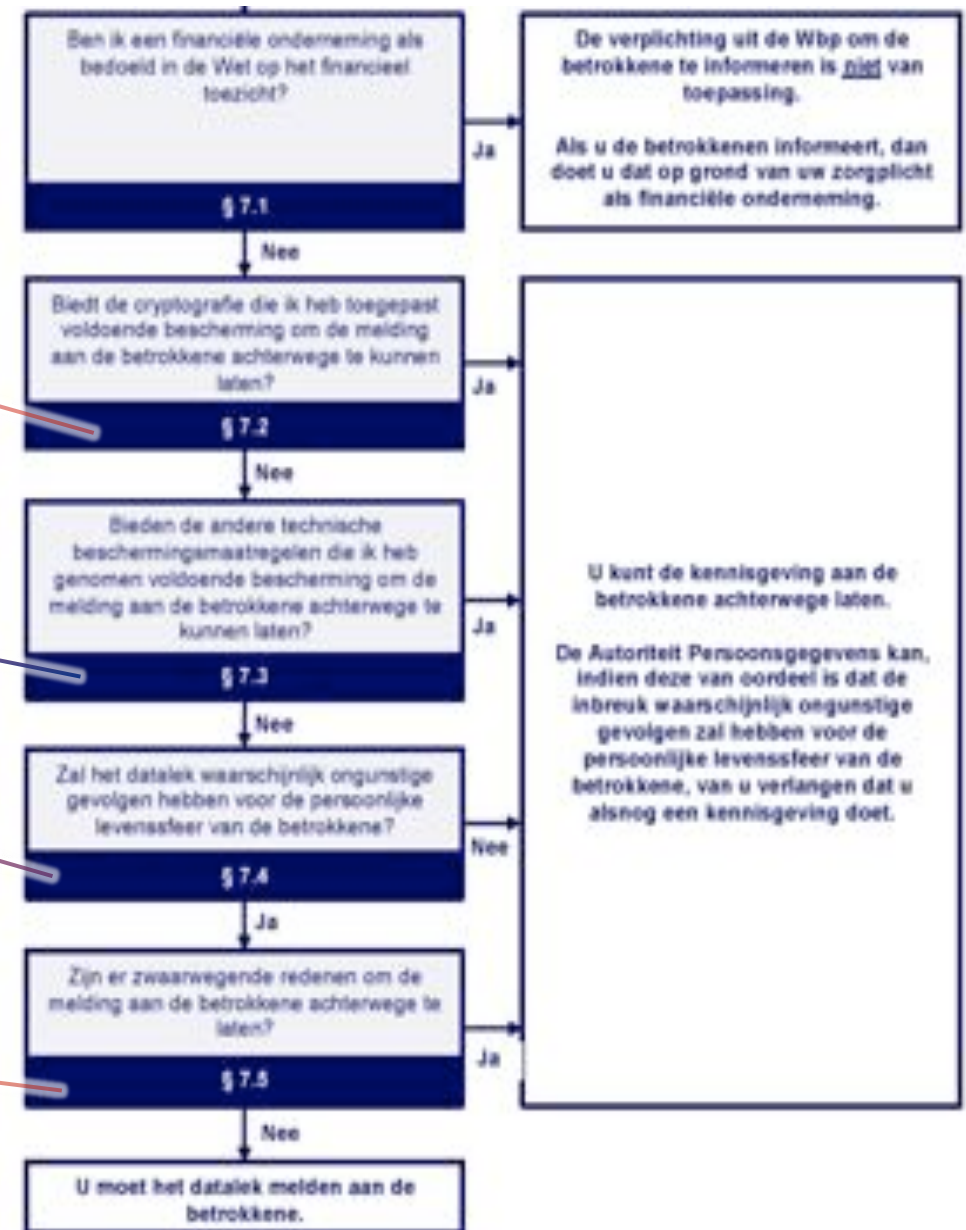
'waarschijnlijk ongunstige gevolgen voor diens persoonlijke levenssfeer'

(art. 34a(6) Wbp) encryptie, hashing beschermt tegen onbevoegde kennisneming (niet tegen vernietiging of aantasting)

bijv. tijdige remote wipe (Mobile-Iron)

risico op schade voor betrokkenen, bijv. identiteitsdiefstal, chantage, aantasting eer en goede naam; bijzondere gegevens of anderzins gevoelige gegevens

*psychosociale hulpvragen van kinderen buiten medeweten van ouders
bedrijfsovername, bank-run*



Meldloket datalekken Autoriteit Persoonsgegevens

Welkom op het meldloket datalekken van de Autoriteit Persoonsgegevens. U kunt hier een melding van een datalek indienen, een bestaande melding aanpassen of een bestaande melding intrekken. Kies hieronder de gewenste actie.

Lees ook onze informatie met betrekking tot [datalekken](#) en de [beleidsregels meldplicht datalekken](#) die hiervoor gelden.

Alle beleidsregels van de Autoriteit Persoonsgegevens zijn te vinden op [deze pagina](#).

Wilt u melding maken van een datalek, maar bent u geen vertegenwoordiger van de organisatie, dan kunt u gebruik maken van ons [tipformulier](#).

Telefonische informatie over de meldplicht datalekken

Op deze website vindt u informatie en antwoorden op vragen over de meldplicht datalekken. Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met de Autoriteit Persoonsgegevens. Het telefoonnummer is 0900-3282535 (voor dit nummer betaalt u uw gebruikelijk tarief voor gesprekken).

U kunt ook een melding indienen, indien uw organisatie een datalek heeft gecorrigeerd.



Meldloket datalekken Autoriteit Persoonsgegevens

Welkom op het meldloket datalekken van de Autoriteit Persoonsgegevens. U kunt hier een melding van een datalek indienen, een bestaande melding aanpassen of een bestaande melding intrekken. Kies hieronder de gewenste actie.

Lees ook onze Informatie met betrekking tot datalekken en de **beleidregels meldplicht datalekken** die hiervoor gelden.

Alle beleidregels van de Autoriteit Persoonsgegevens zijn te vinden op [deze pagina](#).

Wilt u melding maken van een datalek, maar bent u geen vertegenwoordiger van de organisatie, dan kunt u gebruik maken van ons [tipformulier](#).

Telefonische informatie over de meldplicht datalekken

Op deze website vindt u informatie en antwoorden op vragen over de meldplicht datalekken. Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met de Autoriteit Persoonsgegevens. Het telefoonnummer is 0900-3282531 (voor dit nummer betaalt u uw gebruikelijke telefoonkosten).

Kies voor een nieuwe melding indienen, indien uw organisatie een datalek heeft geconstateerd.

[NIEUWE MELDING](#)

Kies voor een bestaande melding aanpassen, indien u een eerder ingediende melding wilt aanpassen of annuleren. Let er op dat u uw meldingsnummer, dat u met het indienen van een nieuwe melding heeft gekregen, moet invullen. Houdt u deze daarom bij de hand.

[BESTAANDE MELDING WIJZIGEN](#)

Kies voor een bestaande melding intrekken, als u een eerder ingediende melding ongedaan wilt maken. Let er op dat u uw meldingsnummer, dat u met het indienen van een nieuwe melding heeft verkregen, moet invullen. Houdt u deze daarom bij de hand.

[MELDING INTREKKEN](#)

Een nieuwe melding indienen

- Naar het melden van een datalek volgt u onderstaand formulier in.
- U dient ieder veld in te vullen.
- Lees ook onze informatie met betrekking tot datalekken.
- Na het indienen wordt een meldingsnummer gegenoteerd ter herkenning. Registreren dit nummer voor toekomstige communicatie met de Autoriteit Persoonsgegevens.

Aard van de melding

Wat is de aard van deze melding?

Wettelijk kader van de melding

Op grond van welke wettelijke bepaling doet u deze melding?

Algemene informatie en contact persoon

Over welk organisatie of bedrijf gaat het?

Naam van het bedrijf of de organisatie

Adres (Bouwlaan) van het bedrijf of de organisatie

Postcode van het bedrijf of de organisatie

Verrijpingsplaats van het bedrijf of de organisatie

Registratienummer bij de Kamer van Koophandel

Door wie wordt het datalek gemeld?

Naam

Functie

E-mailadres

Telefoonnummer

Alternatief telefoonnummer

Met wie kan het CBP contact opnemen voor nadere informatie over de melding?

De mede in contactpersoon

Naam contactpersoon

Functie contactpersoon

E-mailadres contactpersoon

Telefoonnummer contactpersoon

Alternatief telefoonnummer contactpersoon

In welke sector is de organisatie of het bedrijf actief?

Overige sector, te weten:

Gegevens over het datalek

Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.

Werd de inbreuk plaats in een verwerking die is uitbesteed aan een andere organisatie?

Naam van de organisatie waarvan de verwerking is uitbesteed

Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

Is het datalek eenmalig van aard?

Is de datalek voortdurend aanwezig?

Wanneer datum waarop de inbreuk plaats vond

Wat is de aard van de periode waartoe de inbreuk plaats heeft gevonden?

Wat is de aard van de periode waartoe de inbreuk plaats heeft gevonden?

Wanneer werd de inbreuk ontdekt?

Wat is de aard van de inbreuk?

Telefonische informatie over de meldplicht datalekken

Naam

Functie

E-mailadres

Telefoonnummer

Alternatief telefoonnummer

Deze melding persoonsgegevens gaat het?

Telefoonnummer of mobiele telefoon van het bedrijf, indien van toepassing, van de melding

Naam, adres, en woonplaatsgegevens

Geboortedatum

E-mailadres of andere elektronische berichten

Tragings- of identificatiegegevens

Identificatiegegevens

Registratienummer (KVO) of andere nummers

Telefoonnummer of mobiele telefoon van andere personen

Overige gegevens van het bedrijf

Overige persoonsgegevens

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Wanneer is de inbreuk ontstaan?

Is het aanverwante indienen van de melding aan de betrokken autoriteit te laten, namelijk

Ander, namelijk

Technische beschermingsmaatregelen

Zijn de persoonsgegevens versleuteld, gehost of op een andere manier ontzorgd of anderszins beveiligd gemaakt voor onbevoegdheid?

Overige maatregelen

Als de persoonsgegevens geheel of deels ontzorgd of anderszins beveiligd zijn gemaakt, op welke manier is dit gedaan?

Internationale aspecten

Heeft de inbreuk betrekking tot personen in andere EU-landen?

In, namelijk

Heeft uw organisatie, of bedrijf, het datalek gemeld bij beschouwers in een of meer andere EU-landen, of gaat u dat nog doen?

Tuuchthouder(s) van andere landen waar het datalek is gemeld

Vervolgmelding

Is naar uw mening deze melding compleet?

Verhaal de letters en cijfers uit de plaatje. Dit is nodig om misbruik te voorkomen.



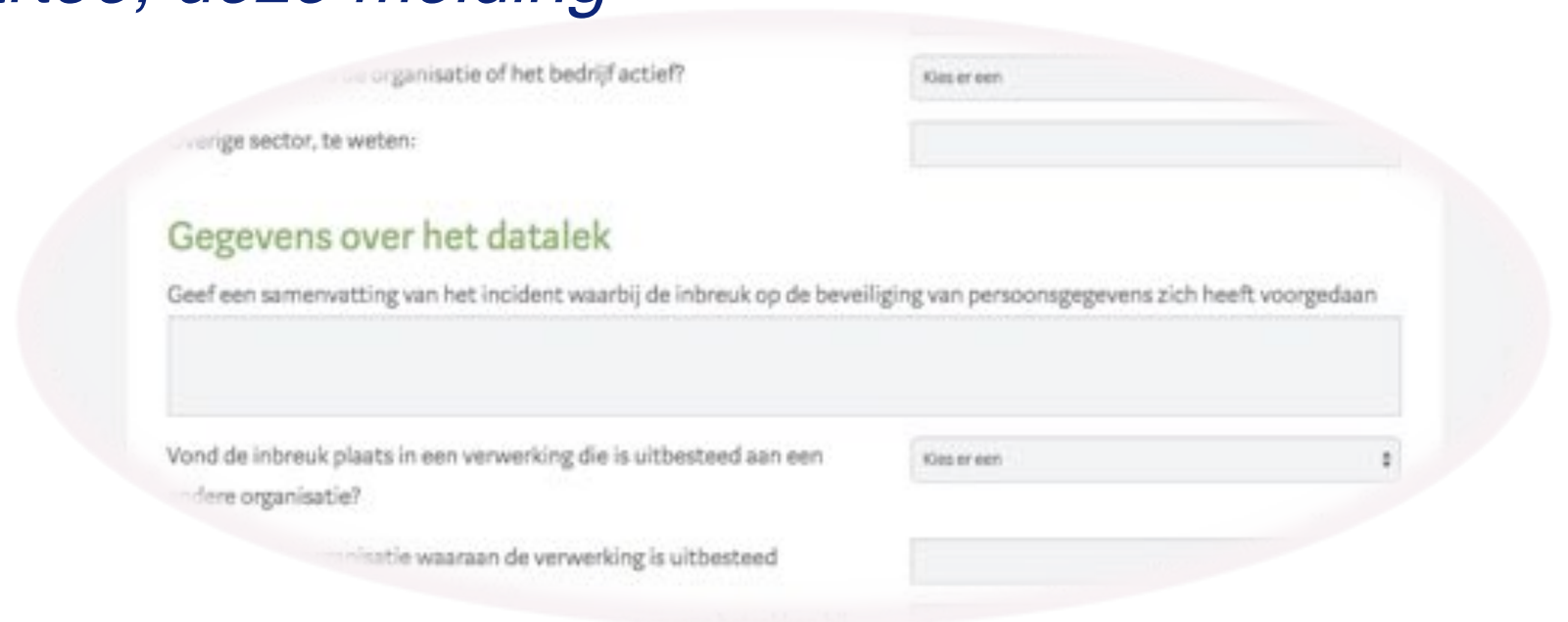
Deur middel van het aanvinken van dit selectievakje verklaart u bezorgd te zijn het het doen van deze melding en dat de in de melding verstrekte informatie juist zijn.

VERSTUREN

authenticatie...? ←

pro forma melding (tekstsuggestie)

“Er is naar oordeel van verantwoordelijke géén sprake van een inbreuk op de beveiliging van de persoonsgegevens. Voor het geval dat daarover verschil van inzicht kan bestaan wordt zekerheidshalve, en zonder aanvaarding van enige gehoudenheid daartoe, deze melding gedaan.”



The image shows a portion of a web form for reporting a data breach. The form is light gray with white text. A large, light pink oval highlights a specific section of the form. The highlighted section is titled "Gegevens over het datalek" in green. Below the title, there is a text input field for a summary of the incident. Above and below this section are other form elements, including dropdown menus and text labels, which are partially obscured or cut off.

...organisatie of het bedrijf actief? Kies er een

...verige sector, te weten:

Gegevens over het datalek

Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan

Vond de inbreuk plaats in een verwerking die is uitbesteed aan een andere organisatie? Kies er een

...organisatie waaraan de verwerking is uitbesteed

C. BESTUURLIJKE BOETEBEVOEGDHEID

bestuurlijke boetes

max. €20.500

- géén vertegenwoordiger aangewezen - art.4(3) Wbp
- doorgifte naar derde land i.s.m. ministeriele regeling – art. 78(2)(a) Wbp



max. €820.000 (of 10% jaaronzet!)

- géén naleving verplichtingen terzake van zorgvuldige verwerking, verwerkingsgrondslagen, doelbinding, bewaartermijn, bewerkers-overeenkomst, **beveiligings- en meldplichten** – art. 6-8, 9(1) en (4), 10(1), 11-13, 34a Wbp
- bijzondere gegevens en BSN – art. 16, 24 Wbp
- informatieplichten, inzage-, verbeterings- en verzetsrechten – art. 33-34(1)-(3), 35(1)-(4), 36(2)-(4), 38-40(2)(3) Wbp
- geautomatiseerde besluitvorming – art. 42(1) en (4) Wbp
- doorgifte derde landen (safe harbor!) – art. 76-77, 78(3) en (4) Wbp

de bindende aanwijzing

- geen bestuurlijke boete dan nadat het een bindende aanwijzing is gegeven
- uitzondering indien de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid

d.w.z. 'zelfstandige last die wegens een overtreding wordt opgelegd' - art. 1(q) Wbp

"ter concretisering van de wettelijke norm [...] aangeven welke gedraging op grond van de Wbp van de overtreder wordt verwacht en hem zo mogelijk moeten opdragen om de overtreding geheel of gedeeltelijk te herstellen"

NvT Boetebeleidsregels én Kamerstukken II 2014/15, 33 662, nr. 9, p. 4.



boetebeleidsregels

- voor beide boetecategorieën onderverdeling naar subcategorieën (I, II of III).
 - per subcategorie een basisboete
 - boeteverlagende en –verhogende omstandigheden
- *recidive*
 - *medewerking aan onderzoek*
 - *op eigen initiatief beëindiging van overtreding*



 @zWenne

vragen?

g.j.zwenne@law.leidenuniv.nl



Universiteit
Leiden

