

PRIVACY AND EU DATA PROTECTION

Seminar XII.

ePRIVACY

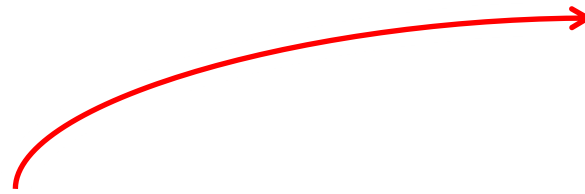
prof. dr. Gerrit-Jan Zwenne

October 9th, 2019



roadmap

- confidentiality of communications



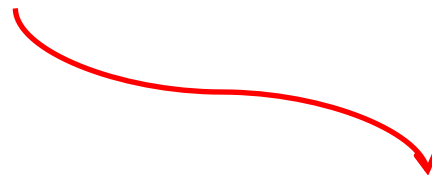
- security obligations (breach notification)
- no tapping, monitoring (eg deep packet inspection)
- requirements re traffic data
- cookies...!

- communication without identification



- directory services ('secret telephone number'), no reversed search
- calling line identification
- not-itemized billing

- unsolicited commercial communications



- spam (e-mail, sms, social networks) and telemarketing

confidentiality of communications

Art. 5 ePR

Art. 4(1) ePD

security obligation

appropriate technical and organisational measures to safeguard **security** of the [electronic communication] services, if necessary in conjunction with the provider of the public communications network with respect to network security

having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

Art. 33-34 GDPR

Art. 4(3) ePD

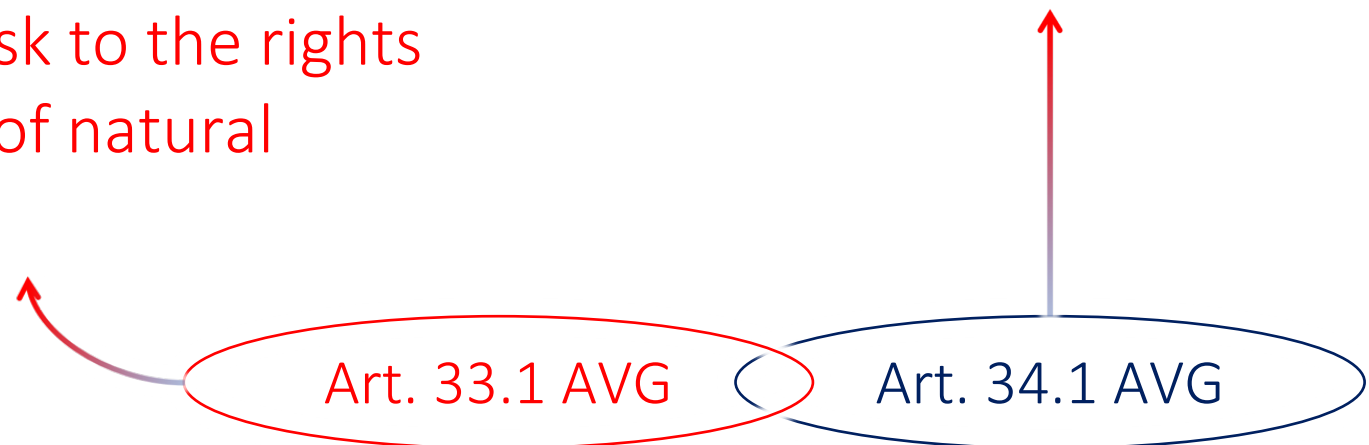
breach notification

- notify the personal data breach to the competent national authority
- also notify the subscriber or individual, if likely to adversely affect the personal data or privacy of a subscriber or individual, of the breach without undue delay

72 hours? what's the startingpoint?

breach notification to DPA
In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority [...], **unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons**

notification to data subject
When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.





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 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 aanvullen. 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

- Voor het melden van een datalek vult 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/bevestiging. Registreer 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 wet(ter) 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 (aanwettelijk) van het bedrijf of de organisatie

Postcode van het bedrijf of de organisatie

Wettingsplaats 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 melder is contactpersoon Ja Nee

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.

Waar is de inbreuk plaats van een verwerking die is uitbesteed aan andere organisaties?

Naam van de organisatie waaraan de verwerking is uitbesteed

Ner minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

Ner maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

Is het bekend wanneer de inbreuk plaats vond? Ja Nee

In welke datum bekend wanneer de inbreuk plaats vond?

Exacte datum waarop de inbreuk plaats vond

Start datum van de periode waartussen de inbreuk plaats heeft gevonden

Eind datum van de periode waartussen de inbreuk plaats heeft gevonden

Wanneer werd de inbreuk ontdekt?

Wat is de aard van de inbreuk?

Selecteer één of meerdere opties (meer dan één mogelijk) Ja Nee

Kapitaal Ja Nee

Verzekeren (zorgverl.) Ja Nee

Verwijden of vernietigen (beschikbaarheid) Ja Nee

Overval Ja Nee

Naar het bekend Ja Nee

Over welk type persoonsgegevens gaat het?

Selecteer één of meerdere opties en geef indien van toepassing een toelichting

Naam, adres en woonplaatsgegevens Ja Nee

Telefoonnummers Ja Nee

E-mailadressen of andere adressen voor elektronische communicatie Ja Nee

Toegang tot identiteitsgegevens Ja Nee

Financiële gegevens Ja Nee

Burgerservicenummer (BSN) of wettnummer Ja Nee

Repasseringspunten of kopieën van andere registratienummers Ja Nee

Overzicht, gegevensbestand en/of bestid Ja Nee

Overige persoonsgegevens Ja Nee

Overige (verbalen)

Wanneer geïnteresserd kan de inbreuk hebben van de persoonlijke levenssfeer van de betrokkene(n)?

Selecteer één of meerdere opties

Identificatie van inbreuk Ja Nee

Schade aan de gezondheid Ja Nee

Wettigheid van (identiteits)gegevens Ja Nee

Wettigheid van open of gesloten Ja Nee

Andere gegevens, namelijk

Vervolgacties naar aanleiding van het datalek

Wanneer technische en organisatorische maatregelen heeft uw organisatie getroffen om de verdere inbreuk te voorkomen?

Heeft u het datalek gemeld aan de betrokkene(n) of bent u van plan dat te gaan doen? Ja Nee

Wanneer heeft u het datalek gemeld aan de betrokkene(n)?

Wanneer gaat u het datalek melden aan de betrokkene(n)?

Wat is de inhoud van de melding aan de betrokkene(n)

Hoeveel betrokkene(n) heeft u in kennis gezet of gaat u in kennis zetten?

Werk communicatiemiddel of welke communicatiemiddel gebruikt u of gaat u te gebruiken?

Als u hebt zwaarwegende redenen om de melding aan de betrokkene achterwege te laten, namelijk

Anders, namelijk

Technische beschermingsmaatregelen

Zijn de persoonsgegevens versleuteld, gehesit of op een andere manier onbegrijpelijk of onontzorgelijk gemaakt voor onbetrokken?

Deels, namelijk

Als de persoonsgegevens geheel of deels onbegrijpelijk of onontzorgelijk zijn gemaakt, op welke manier is dit dan gebeurd?

Internationale aspecten

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

Ja, namelijk

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

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

Vervolgmelding

Is naar uw mening deze melding compleet?

Herhaal de letters en cijfers uit dit veldje. Dit is nodig om misbruik te voorkomen.

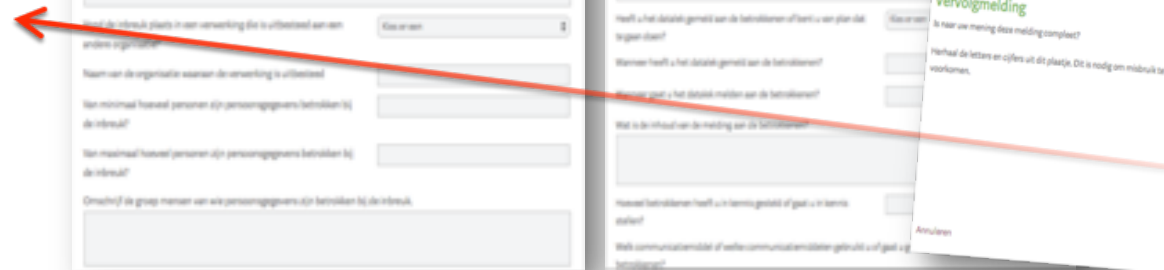
Amnulen

fm882

Door middel van het aanvulven van dit selectievakje verklaart u bevestigd te zijn tot het doen van deze melding en dat de in de melding verstrekte inlichtingen juist zijn.

VERSTUREN

authentication...?



“electronic communications
metadata”

Art. 6 ePR

Art. 5(1) ePD

confidentiality of communications
and traffic data

no listening, tapping, storage or
other kinds of interception or
surveillance of communications
and the related traffic data by
persons other than users, without
the consent of the users
concerned

*deep packet
inspection (“dpi”)*

*net neutrality
debat...*

spam filter..?

communication without identification

traffic data relating to subscribers and users must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication



with user or subscriber consent data may be used for the purpose of marketing electronic communications services or for the provision of value added services

cookies! device fingerprinting,
pixels etc..

Art. 8 ePR

Art. 5(3) ePD

the storing of information, or the gaining of
access to information already stored, in the
terminal equipment of a subscriber or user is
only allowed on condition that the subscriber
or user concerned has given his or her consent,
having been provided with clear and
comprehensive information

“cookies”

but functional or technical cookies are allowed
nevertheless

where technically possible and feasible [...] consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.

subscriber has the right to have
invoice without details



non-itemized billing

calling line identification

directory services



- subscriber must be informed about inclusion in directories (incl purposes), and
- provided a choice (opt-in or opt-out)

Art. 7, 8 and 12 ePD



user has the right to

- block cli-presentation of his/her own calls
- reject cli-blocked calls from others
- block cli-presentation of calls from others

unsolicited commercial communication

Art. 13 ePD

exemption for own similar products and services

who is (are) sender(s) in the context of affiliates networks?
what is commercial?

opt-in for

- automated calling (communication) devices
- commercial fax and e-mail

opt-out for

- telemarketing

exemption for own similar products and services

do-not-call register
outbound and inbound?

questions?

g.j.zwenne@law.leidenuniv.nl