

LAW AND DIGITAL TECHNOLOGIES
ELECTRONIC COMMUNICATIONS

ePrivacy

Prof. Gerrit-Jan Zwenne
February 12th, 2020



roadmap

- confidentiality of communications
- communication without identification
- unsolicited commercial communications

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

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

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

subscriber



user



end-user





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, f the breach without undue delay

*24 hours? 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.

Security

Gemalto: NSA, GCHQ hacked us – but didn't snatch crucial SIM keys

'Investigation' admits to attacks, but says phone crypto secrets stayed secure

25 Feb 2015 at 08:00, Simon Sharwood



31



Gemalto, the world's biggest SIM card maker, has investigated the NSA's and GCHQ's infiltration of its computers – and says that while the agencies did get into its network, they didn't get in far enough to siphon off phone-call encryption keys.

Files leaked by intelligence whistleblower Edward Snowden [appeared to show](#) the US and UK had broken into Gemalto's systems to obtain thousands, if not millions, of secret encryption keys (K_i) which are baked into every SIM – and used to safeguard conversations from eavesdroppers.



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 bent ieder weld in de wijzen.
- Lees ook onze informatie met betrekking tot [datalekken](#).
- Na het indienen wordt een meldingsnummer getoond ter bevestiging. Registreren dit nummer voor toekomstige communicatie met de Autoriteit Persoonsgegevens.

Aard van de melding

Wat is de strekking van deze melding?

Nieuwe melding

Wettelijk kader van de melding

Op grond van welke wettelijke bepaling doet u deze melding?

Kies er een

Algemene informatie en contactpersoon

Over welk organisatie of bedrijf gaat het?

Naam van het bedrijf of de organisatie

Adres (zoekenadres) van het bedrijf of de organisatie

Postcode van het bedrijf of de organisatie

Wettelijke plaats 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?

Kies er een

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

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

Kies er een

Naam van de organisatie waaraan de verwerking is uitbesteed

Van minimaal hoeveel personen zijn persoonsgegevens betroffen bij de inbreuk?

Van maximaal hoeveel personen zijn persoonsgegevens betroffen bij de inbreuk?

Omvat het de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

Is het bekend wanneer de inbreuk plaats vond?

☐ Ja ☐ Nee

Is de exacte datum bekend wanneer de inbreuk plaats vond?

☐ Ja ☐ Nee

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

Lezen (vertrouwelijkheids)

☐ Ja ☐ Nee

Kopieren

☐ Ja ☐ Nee

Veranderen (integriteit)

☐ Ja ☐ Nee

Verwijderen of vernietigen (beschikbaarheid)

☐ Ja ☐ Nee

Diefstal

☐ Ja ☐ Nee

Nog niet bekend

☐ Ja ☐ Nee

Om welk type persoonsgegevens gaat het?

Selecteer één of meerdere opties en geef, indien van toepassing, een beschrijving

Naam, adres en woonplaatsgegevens

☐ Ja ☐ Nee

Telefoonnummers

☐ Ja ☐ Nee

E-mailadressen of andere adressen voor elektronische communicatie

☐ Ja ☐ Nee

Toegangs- of identiteitsgegevens

☐ Ja ☐ Nee

Financiële gegevens

☐ Ja ☐ Nee

Burgerservicenummer (BSN) of voornummer

☐ Ja ☐ Nee

Rechtsgegevens of kopieën van andere legitimatiebewijzen

☐ Ja ☐ Nee

Geslacht, geboortedatum en/of leeftijd

☐ Ja ☐ Nee

Bijzondere persoonsgegevens

☐ Ja ☐ Nee

Overige inbreuk

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkene(n)?

Selecteer één of meerdere opties

Stigmatisering of uitsluiting

☐ Ja ☐ Nee

Schade aan de gezondheid

☐ Ja ☐ Nee

Wettelijke aansprakelijkheid

☐ Ja ☐ Nee

Wettelijke aansprakelijkheid

☐ Ja ☐ Nee

Andere gevolgen, namelijk:

Vervolgacties naar aanleiding van het datalek

Welke 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?

Kies er een

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 gesteld of gaat u in kennis stellen?

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken?

Technische beschermingsmaatregelen

Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontegenwoordig gemaakt voor onbevoegden?

Kies er een

Deels, namelijk:

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

Internationale aspecten

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

Ja, namelijk:

Kies er een

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 plaatje. Dit is nodig om misbruik te voorkomen.

Kies er een



Door middel van het aanvinken van dit selectievakje verklaart u bevoegd te zijn tot het doen van deze melding en dat de in de melding verstreepte inlichtingen juist zijn.

Annuleren

VERSTUREN

authentication...?

Art. 6 EPR

Art. 5(1) ePD

*“electronic
communications
metadata”*

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..?

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 data may be used for the purpose of marketing electronic communications services or for the provision of value added services.

2006/24/EC

*processed and stored by the
provider of a public
communications network or
publicly available electronic
communications service*

6 to 24 months

data retention obligation for the
purpose of the investigation, detection
and prosecution of serious crime

*as defined by each Member
State in its national law*

*Data Retention Directive
2006/24/EC annulled by CJEU 8
April 2014 C-293/12 and C-594/12*

Art. 8 ePR

Art. 5(3) ePD

*cookies! device fingerprinting,
pixels etc..*



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*

*Consent should not be regarded as
freely given if the data subject has
no genuine or free choice or is
unable to refuse or withdraw
consent without detriment*

pop-ups or banner

explicit or implied consent

commercial tracking cookies

cookie retention terms

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

communication without identification

*subscriber has the right to have
invoice without details*



non-itemized billing

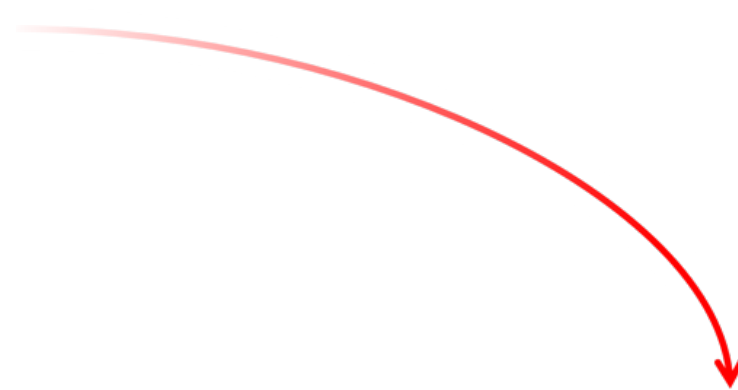
calling line identification

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?

exemption for own similar products and services

opt-in for

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

opt-out for

- telemarketing

do-not-call register
outbound and inbound?

questions?

g.j.zwenne@law.leidenuniv.nl

