Ministerie van
Economische Zaken

BEWAARPLICHT TELECOMMUNICATIE-GEGEVENS

14 oktober 2009

Ministerie van
Economische Zaken

PROGRAMMA

- TOELICHTING OP WET EN DE BEHANDELING IN DE KAMER
- VERGOEDINGEN
- TOEZICHT, HANDHAVING
- PROJECT HISTORISCHE VERKEERSGEGEVENS
- DEELPROJECT HISTORISCHE NAW
- STANDAARDEN
- DISCUSSIE / DEBAT?
- AFSLUITING

Ministerie van
Economische Zaken

BEWAARPLICHT TELECOMMUNICATIE-GEGEVENS

14 oktober 2009

Ministerie van Justitie

Wet bewaarplicht telecommunicatie

Bob Stap

Ministerie van Justitie

Wet bewaarplicht telecommunicatie
14 oktober 2009

Wat is hieraan vooraf gegaan

- EU Richtlijn dataretentie
  van 15 maart 2006
- Bewaartermijn van 6 tot 24 maanden

Parlementaire behandeling

- Nut en noodzaak
- Privacy
- Kosten
- Beeldvorming
  - ICT mogelijkheden
  - vertrouwen in de overheid

Wat moet bewaard worden

- Gegevens die nodig zijn om de **bron** van de communicatie te traceren en te identificeren
- Gegevens die nodig zijn om de **bestemming** van een communicatie te identificeren
- Gegevens die nodig zijn om **datum**, **duur** en **tijdstip** van de communicatie te bepalen
- Gegevens die nodig zijn om het **type communicatie** te bepalen
- Gegevens die nodig zijn om de **communicatieapparatuur** van de gebruikers te identificeren
- Gegevens die nodig zijn om de **locatie** van mobiele apparatuur te bepalen

Wat moet bewaard worden

- Aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten bewaren de in de bij deze wet behorende bijlage aangewezen gegevens, voorzover deze in het kader van de aangeboden netwerken of diensten worden gegenereerd of verwerkt, ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven.

Ministerie van
Economische Zaken

BEWAARPLICHT TELECOMMUNICATIE-GEGEVENS

14 oktober 2009

Kostenvergoeding bij informatieverstrekking

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Joost Bruinsma

Kostenregeling

Op basis van 13.6 Telecomwet is er een ministeriële regeling m.b.t. de vaststelling en vergoeding van de personeels- en administratiekosten kosten (Stass EZ)

volgens indicatief tarief

voor zover kosten in redelijkheid als noodzakelijk kunnen worden beschouwd

met een groep van aanbieders kunnen afspraken worden gemaakt over de hoogte van de vergoeding en de voorwaarden voor uitbetaling.

Uitgangspunten evt. uitbreiding/aanpassing

Aansluiten bij huidige kostenregeling

Uitgangspunten:

- Verlichten van de uitvoeringslasten bij informatieverstrekking
- Waarborgen van de kwaliteit
- Administratieve lasten beperken
- Binnen een korte termijn te realiseren

Denkrichting

Dienstverlenermodel

Kosten voor inschakelen (extra) dienstverlener worden aangemerkt als redelijk gemaakte kosten

Dienstverlener kan een maximaal vast te stellen bedrag declareren bij de overheid.

Markt is vrij in het zoeken van eigen/betere oplossingen en het creëren van dienstverleners.

Voordelen

-Verlichten van de uitvoeringslasten bij informatieverstrekking en kostenreductie

Helderheid over de mogelijkheden om de noodzakelijk gemaakte kosten te declareren

Eenvoudiger om aan de wettelijke gestelde kwaliteitseisen te voldoen

Minder administratieve lasten

Vervolgstappen

- (Financiële) consequenties *dienstverlenermodel* worden onderzocht

- Technische specificaties en eisen moeten worden uitgewerkt

- Input van vandaag
  - Suggesties zijn welkom!
  - Consultatie marktpartijen najaar 2009
  - Aangepaste regelgeving in de loop van 2010 (indien noodzakelijk)

Ministerie van
Economische Zaken

BEWAARPLICHT TELECOMMUNICATIE-GEGEVENS

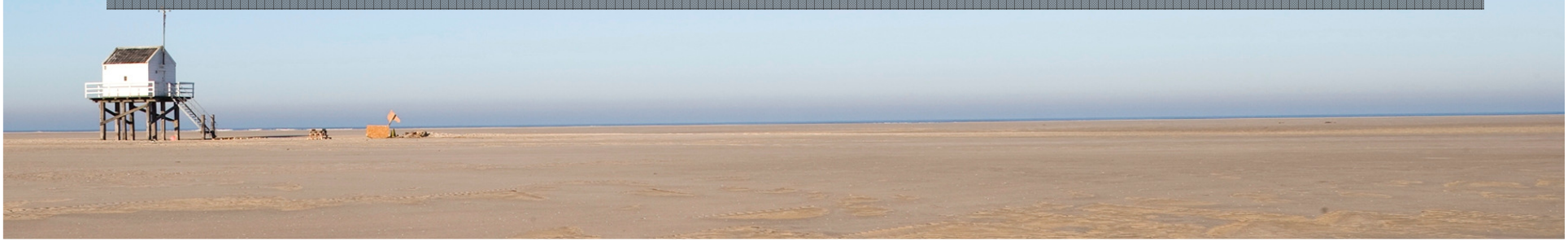
14 oktober 2009

Toezicht op de Bewaarplicht van Telecommunicatiegegevens

Aad Oosthoek
Agentschap Telecom

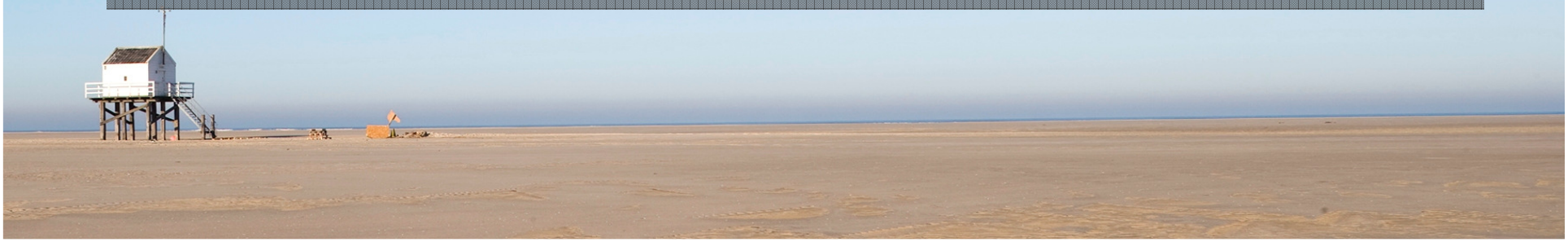
Inhoud presentatie

1. Agentschap Telecom
2. Fasering toezicht
3. Overtredingen
4. Nulmeting



Agentschap Telecom

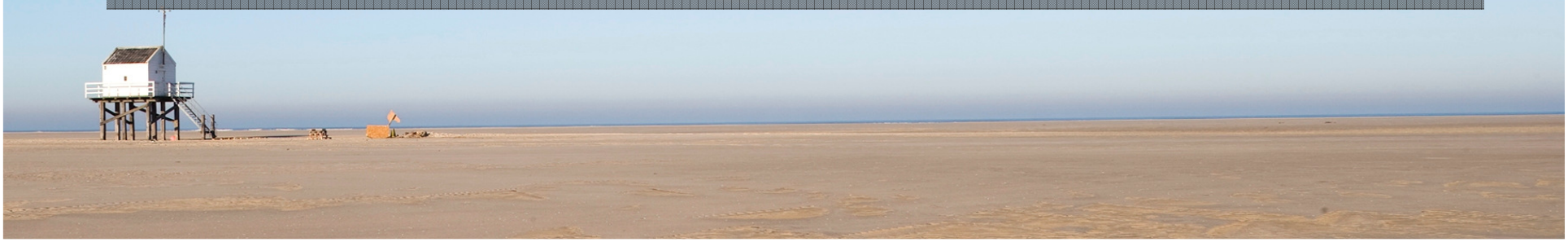
- ✓ Onafhankelijk Toezichthouder
- ✓ Onderdeel Ministerie van Economische Zaken
- ✓ Legt verantwoording af aan de Staatssecretaris van Economische Zaken



De rol van Agentschap Telecom bij Dataretentie

1. Houdt toezicht op naleving wet- en regelgeving dataretentie

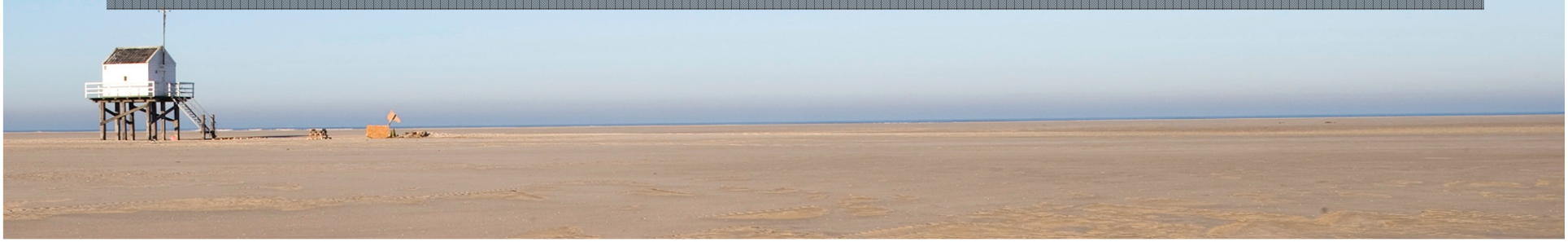
2. Treedt desgevraagd op bij geschillen tussen aanbieder en behoeftesteller



De rol van Agentschap Telecom

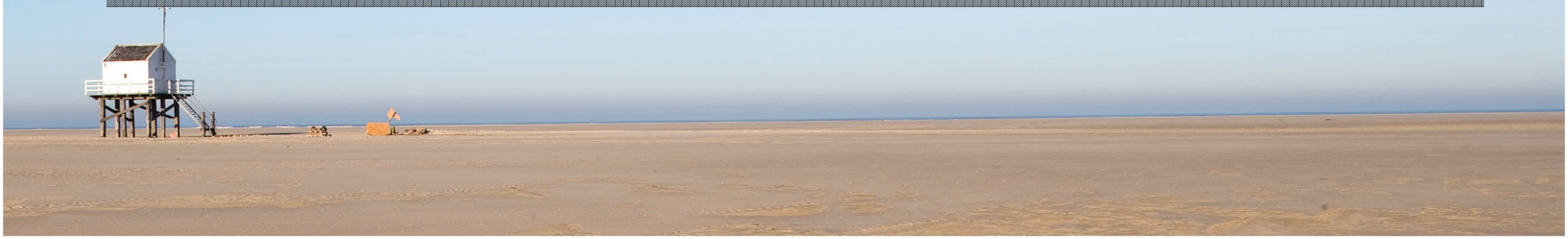
Ook toezicht op naleving van onder meer

1. Vernietigen van telecommunicatiegegevens
2. Bevoegd aftappen



Doel van het Toezicht

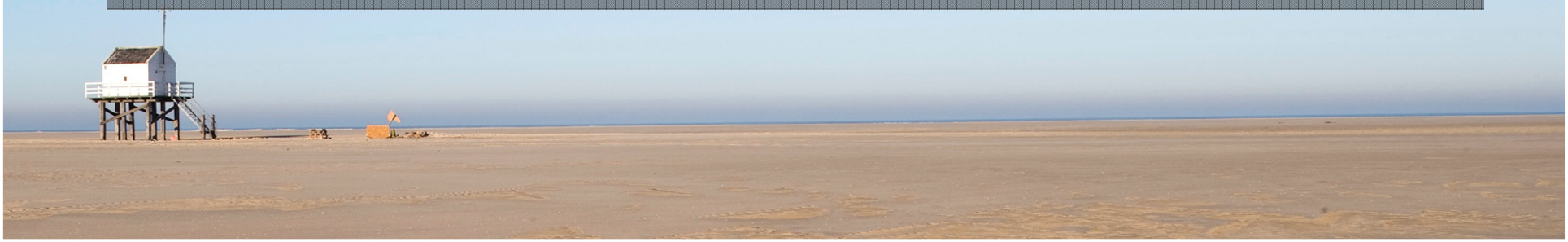
Het risico op incidenten en mogelijke schade door overtredingen zo klein mogelijk houden.



Fasering van de invoering van het toezicht

Het eerste toezichtsjaar

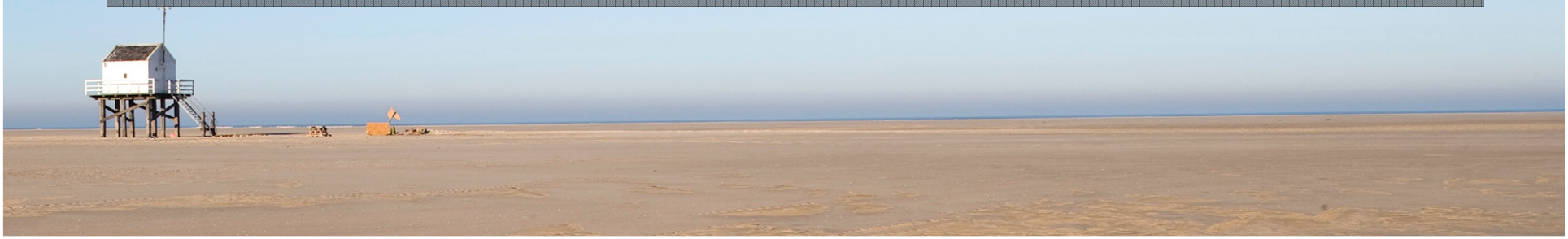
- Voorlichting
- Nulmeting
- Opsturen beveiligingsplan
- Coulance ten aanzien van het weten en kunnen
- Geen coulance bij niet-willen



Fasering van de invoering van het toezicht

Het tweede toezichtjaar

- Risico analyse
- Differentiatie in toezicht
- Aanscherping toezicht
- Evaluatie toezicht

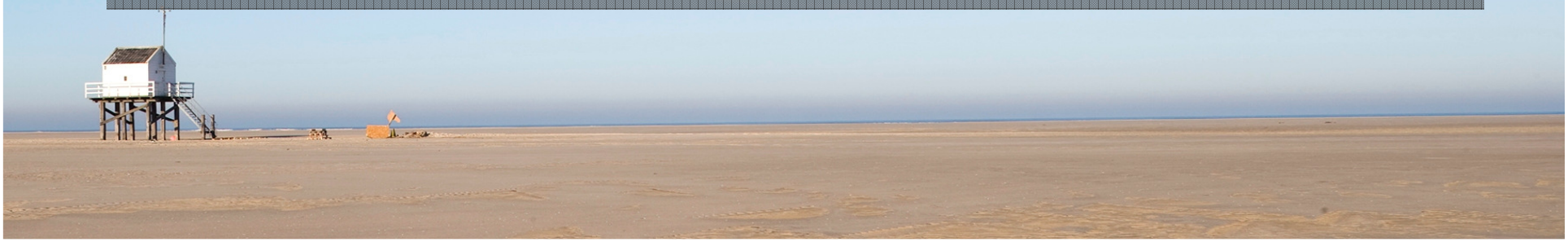


Uitgangspunt bij het toezicht

Agentschap Telecom hanteert het volgende uitgangspunt:

Het gaat al snel om geautomatiseerde verwerking van gegevens. Dus:

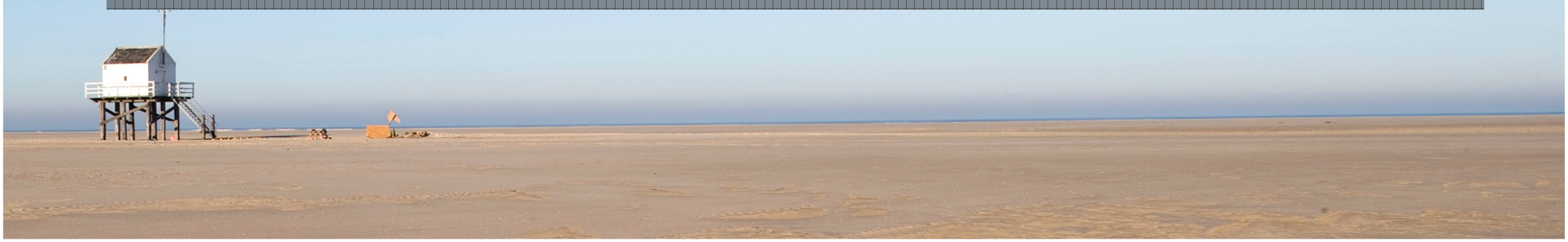
- Schrijf op wat je doet
- Doe wat je opgeschreven hebt
- Laat zien dat het zo gegaan is



Wat zijn de gevolgen bij een overtreding?

Agentschap Telecom hanteert volgende interventies bij overtredingen:

- waarschuwing
- last onder dwangsom
- boete
- strafrecht



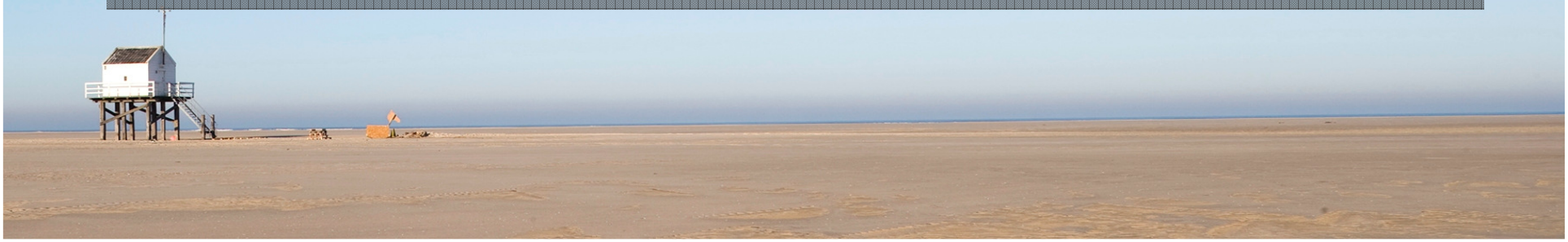
Wat zijn de gevolgen bij een overtreding?

Factoren van belang bij bepalen sanctie:

Overtredingen bewaarplicht onderscheiden in:

1. Lichte overtredingen
2. Middelzware overtredingen
3. Zware overtredingen

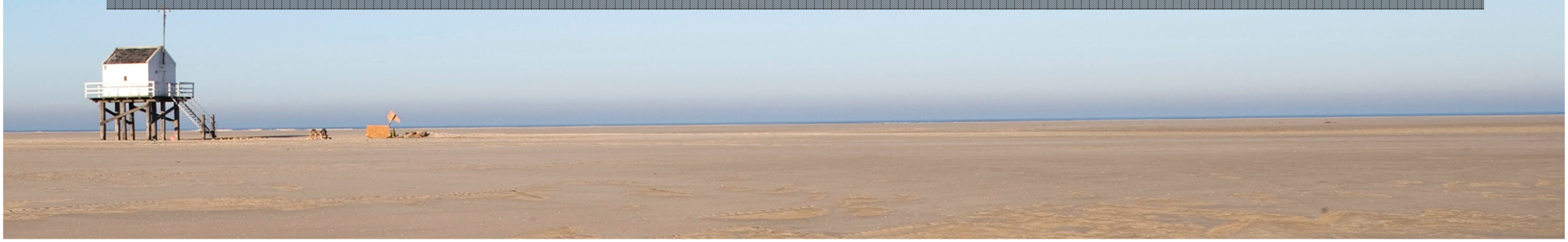
Omvang aanbieder bepalend voor hoogte sanctie



Nulmeting

Toezegging minister van Justitie aan Eerste Kamer m.b.t. de nulmeting:

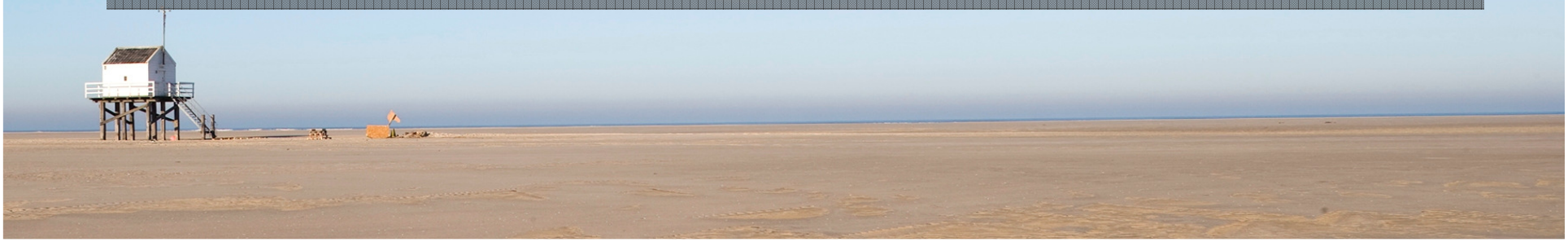
- IST situatie
- Beveiliging gewaarborgd
- Proportionaliteit investeringskosten



Nulmeting

- Vragenbrief aan aanbieders verzonden
- Toetsing beveiligingsplannen
- Analyse antwoorden

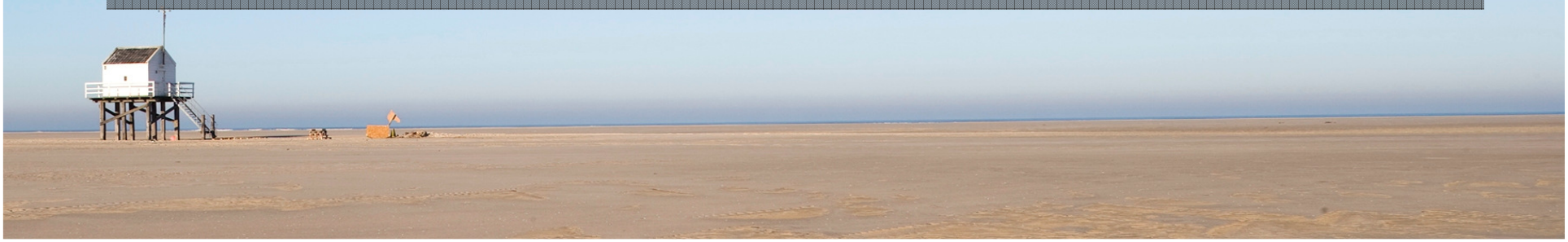
- Prioritering op basis risicoanalyse
- Fysieke inspecties
- Eindrapportage aan Eerste Kamer april 2010



Tot slot

- Meer informatie vindt u op www.agentschaptelecom.nl.

  en in de Wet zelf: kijk daarvoor op www.wetten.nl.



Tot slot

Dank voor uw aandacht

Heeft u vragen of opmerkingen?

informatieveiligheid@at-ez.nl

Ministerie van
Economische Zaken

BEWAARPLICHT TELECOMMUNICATIE-GEGEVENS

14 oktober 2009

Ministerie van Justitie

Project Data-Retentie
& onderzoek Historische Verkeersgegevens

Informatiebijeenkomst

14 oktober 2009

Presentatie 14 oktober 2009

- Toelichting project Data-Retentie

- Aanleiding, doel, resultaten
- Organisatie & rol aanbieders
- Projectopzet –en planning

- Onderzoek Historische Verkeersgegevens (HVG)

- Doel, resultaten
- Organisatie & rol aanbieders
- Planning

Opdracht project Data-Retentie

Aanleiding

- Wetgeving Data-Retentie
- Er bestaan veel verschillende communicatielijnen bij dit proces aangezien er een groot aantal organisaties zijn betrokken (bij zowel overheid als aanbieders)
- De overheid wil het bestaande proces m.b.t. het opvragen van gegevens bij de aanbieders effectiever en efficiënter inrichten
- De focus van efficiëntie (en effectiviteit) ligt bij zowel de overheid als bij de aanbieders
- De overheid wil hiervoor de mogelijkheden inventariseren om efficiëntie te bereiken door geautomatiseerd aanleveren van gegevens via een informatiemakelaar

Opdracht project Data-Retentie

Doel

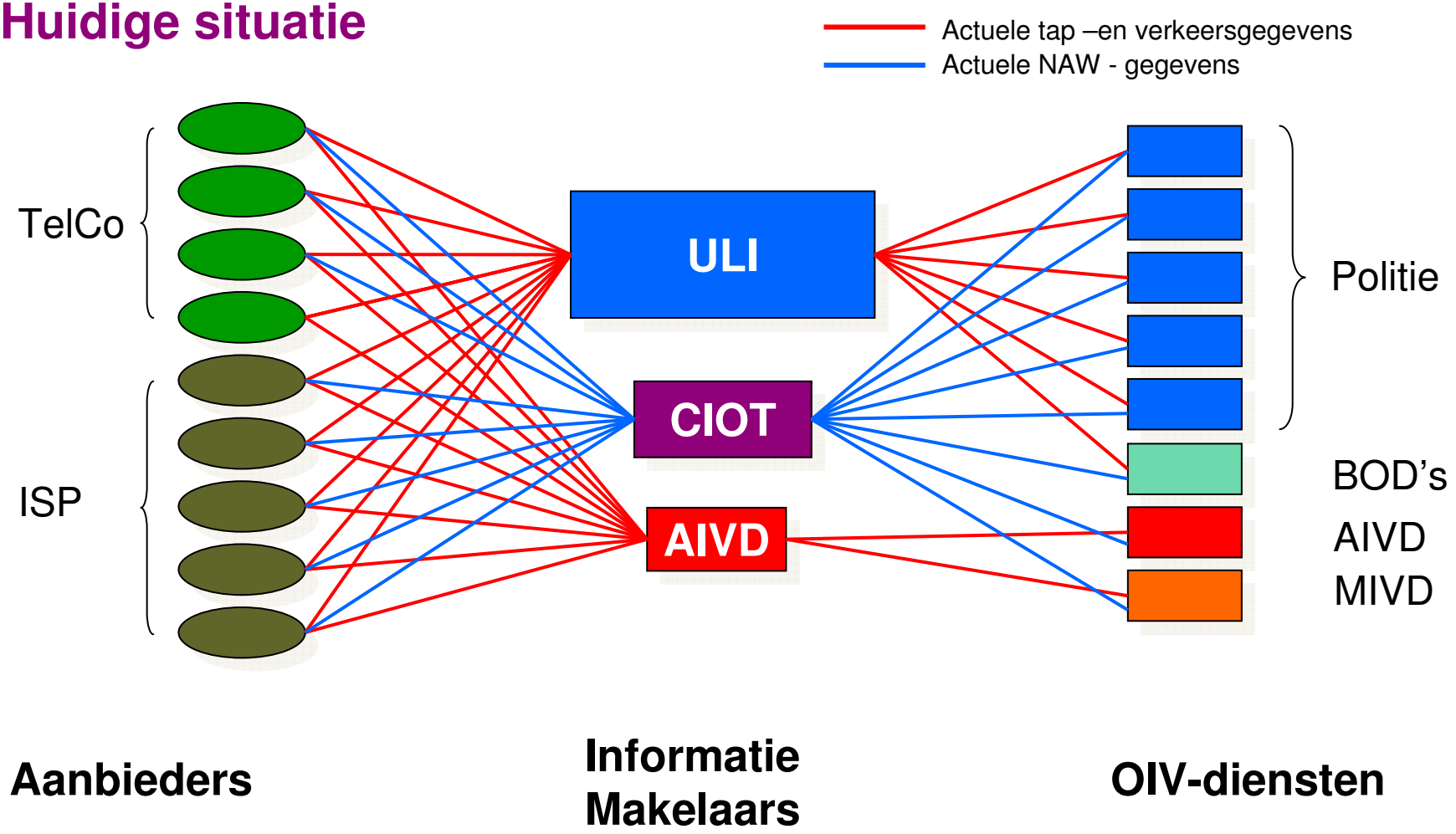
- Alternatieve haalbare voorstellen ontwikkelen om historische verkeersgegevens (HVG) en de historische NAW-gegevens (HNAW) voor de I&V-en opsporingsdiensten geautomatiseerd aan te leveren. De financiële dekking dient in deze voorstellen meegenomen te worden. Ook dient er uitgegaan te worden van de goede ervaringen van het CIOT model.

Resultaten

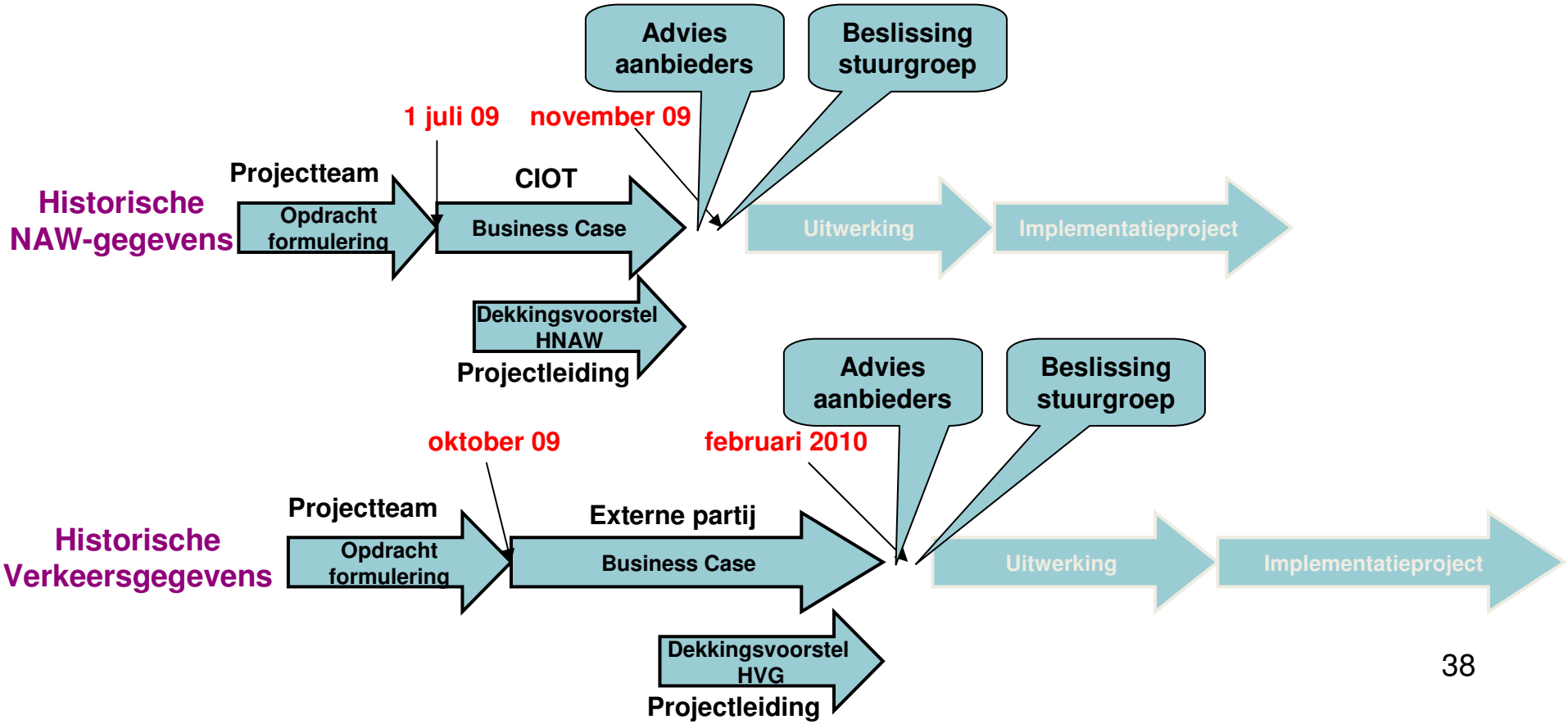
1. Business Case voor Historische NAW gegevens (HNAW)
2. voorstel voor de financiële dekking van deze BC HNAW
3. Business Case voor Historische Verkeersgegevens (HVG)
4. voorstel voor de financiële dekking van deze BC HVG

Randvoorwaarden

Huidige situatie

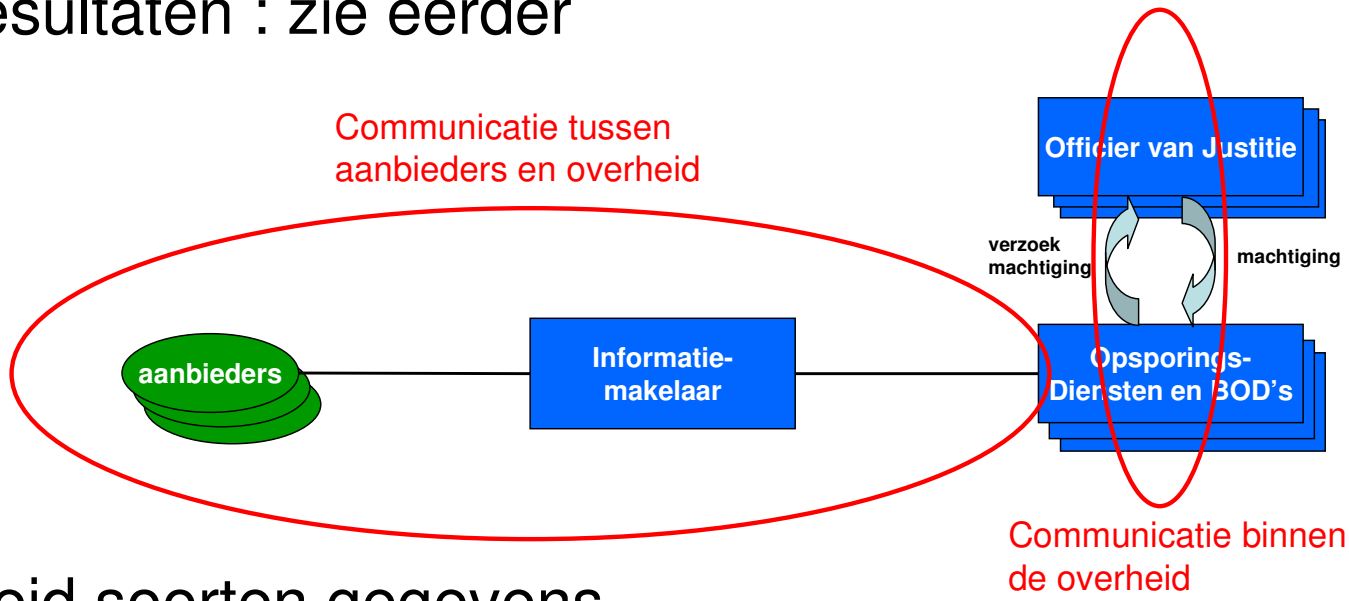


Project opzet en fasering



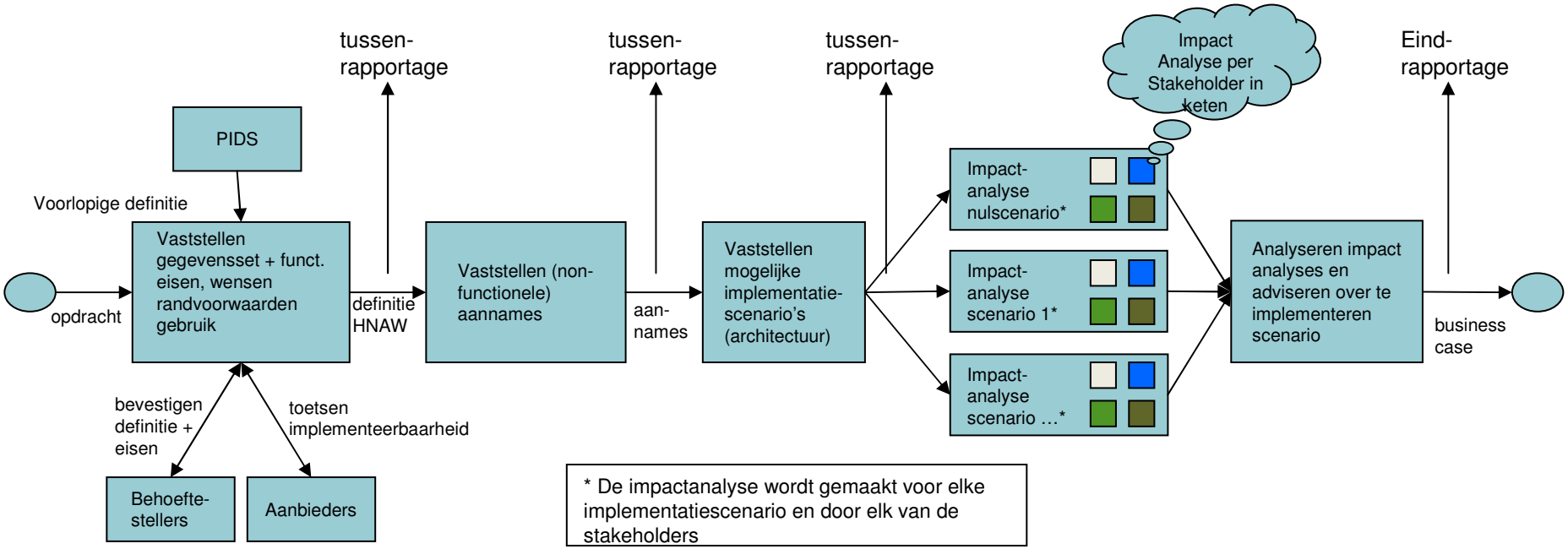
Onderzoek Historische Verkeersgegevens

- Doel en resultaten : zie eerder
- Scope:



- Onderscheid soorten gegevens
- Extern bureau

Stappenplan Business Case HVG



Organisatie

- Opdrachtgever : project Data-Retentie
- Uitvoering: extern bureau
- Betrokkenen
  - Alle overheidspartijen
  - Aanbieders tijdens proces (vorm wordt nog bepaald)
- Advies over eindvoorstel (concept Business Case)

Planningsoverzicht project & HVG

Mijlpaal	
Opdracht voor Business Case (BC) HNAW	jul-09
Oplevering Concept Business Case (BC) HNAW	nov-09
Dekkingsvoorstel voor BC HNAW	nov-09
Advies aanbieders	dec-09
Go – No Go door Stuurgroep HNAW	**dec-09**
Opdracht voor Business Case (BC) HVG	okt-09
Opdracht extern onderzoek	okt-09
Oplevering Concept Business Case (BC) HVG	feb-10
Dekkingsvoorstel voor BC HVG	feb-10
Advies aanbieders	mrt-10
Go – No Go door Stuurgroep HVG	**mrt-10**

Ministerie van Justitie

Project Historische NAW

René Bladder (CIOT)

CIOT- Centraal Informatiepunt Onderzoek Telecommunicatie

Middel voor aanbieders opsporingsvragen te beantwoorden;

- Met toezicht op het gebruik;
- En onafhankelijke audits;
- Efficiënt en effectief.

Geeft alleen antwoord op de vragen:

- Welke persoon of aanbieder hoort nu bij een nummer;
- Welke nummers horen nu bij een bepaald persoon;

Opdracht project HNAW

Ontwikkel een *haalbaar* voorstel, in de vorm van een Business Case,

waarmee de HNAW gegevens van de Telecom en ISP aanbieders

effectief en efficiënt voor de opsporingsdoeleinden kunnen worden ontsloten.

Resultaat project HNAW

- Inventarisatie aannames, eisen & wensen en randvoorwaarden onder stakeholders;

- Beschrijven implementatiescenario's:
  - Historische bevraging op de huidige manier;
  - Uitbreiden huidige NAW oplossing met Historische NAW gegevens en deze bevraagbaar maken;
  - Anders?

- Uitvoeren risico en impact analyse om voorkeurscenario vast te stellen en op te nemen in Business Case HNAW

- De stuurgroep Dataretentie stelt het vervolgtraject vast.

HNAW Aanpak

HEDEN

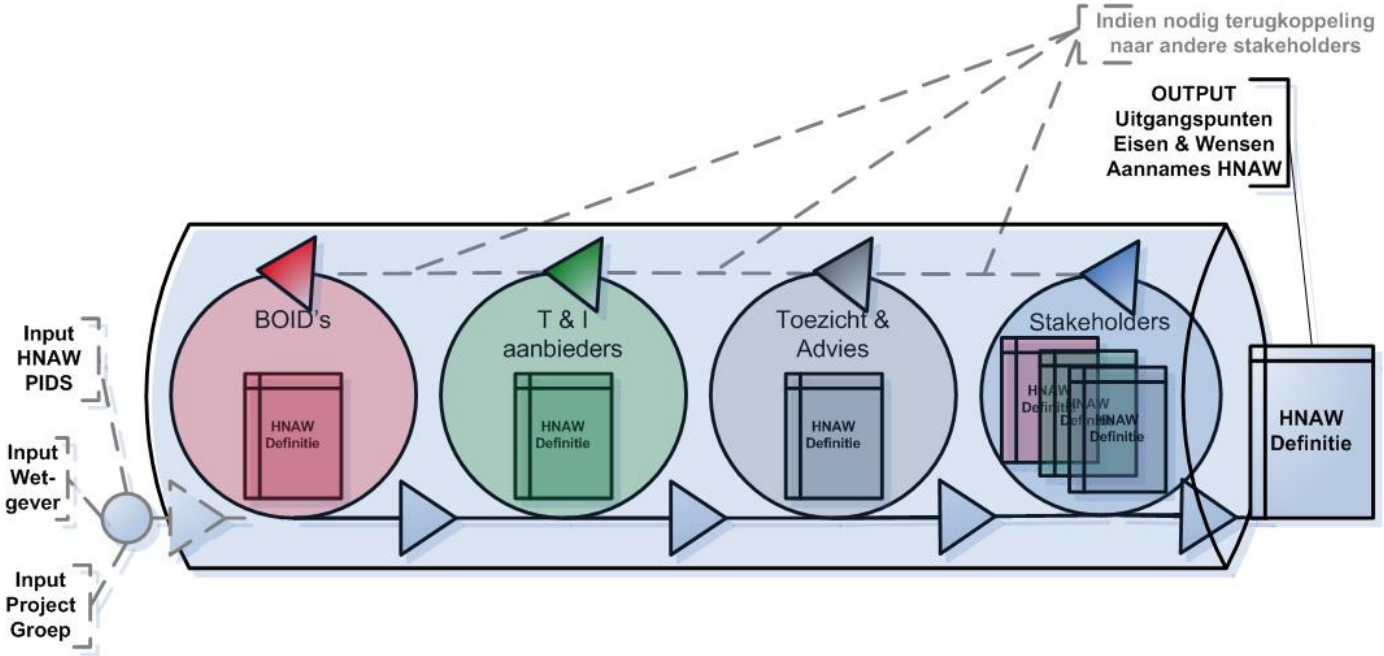
NAW + Historische NAW

GEWENST

Historische NAW

WIJZIGING

BC: VAN-NAAR beschrijving



Vervolg project HNAW

oktober

week	40	41	42	43	44
m		5	12	19	26
d		6	13	20	27
w		7	14	21	28
d	1	8	15	22	29
v	2	9	16	23	30
z	3	10	17	24	31
z	4	11	18	25	

Donderdag 22 oktober a.s.

Aanbiedersbijeenkomst HNAW in UTRECHT

Uitnodiging per mail verstuurd

Einde

Bedankt voor uw aandacht.

René Bladder
070-3703310
http://www.ciot.nl

Ministerie van
Economische Zaken

BEWAARPLICHT TELECOMMUNICATIE-GEGEVENS

14 oktober 2009

Ministerie van Economische Zaken

Informatiebijeenkomst bewaren telecommunicatiegegevens

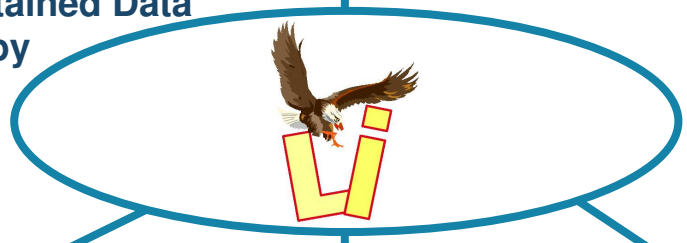
ETSI activities on standardisation of Data Retention handling

Peter van der Arend
Chairman ETSI/TC LI
(Technical Committee on Lawful Interception)

European
Telecommunications
Standards
Institute

Handover Interfaces for transport of
Lawful Interception and Retained Data
are standardised by

Technical Committee



Lawful Interception

Lawful Interception

Security LI & RD
environment

Retained Data

Why study on Retained Data in EU

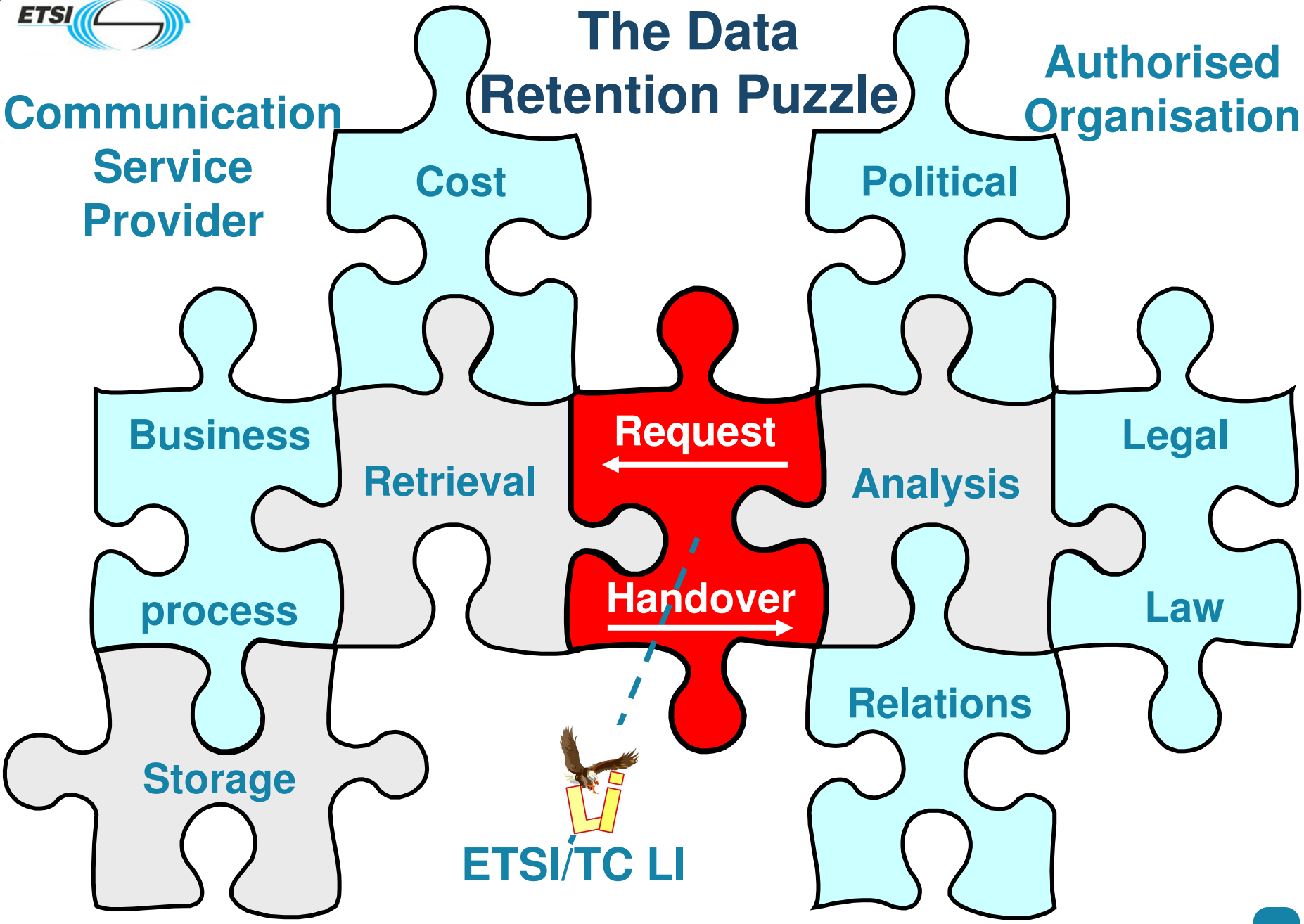
15th of March 2006: the European Parliament and the Council of the European Union adopted Directive 2006/24/EC on Data Retention

Data generated or processed in connection with the provision of publicly available electronic communications services
or of
public communications networks
need to be retained

Applicability Directive

- The content of the communication is not part of the directive
- Data to be Retained
  - Successful and unsuccessful communication attempts
  - Wireline network telephony / Wireless network telephony
  - Internet access / Internet e-mail / Internet telephony
- Categories of data to be retained
  - data to trace and identify the source of a communication
  - data to identify the destination of a communication
  - data to identify the date, time and duration of a communication
  - data to identify the type of communication
  - data to identify users' communication equipment or what purports to be their equipment
  - data to identify the location of mobile communication equipment
- Proportional requirements shall be defined by each Member State in its national law

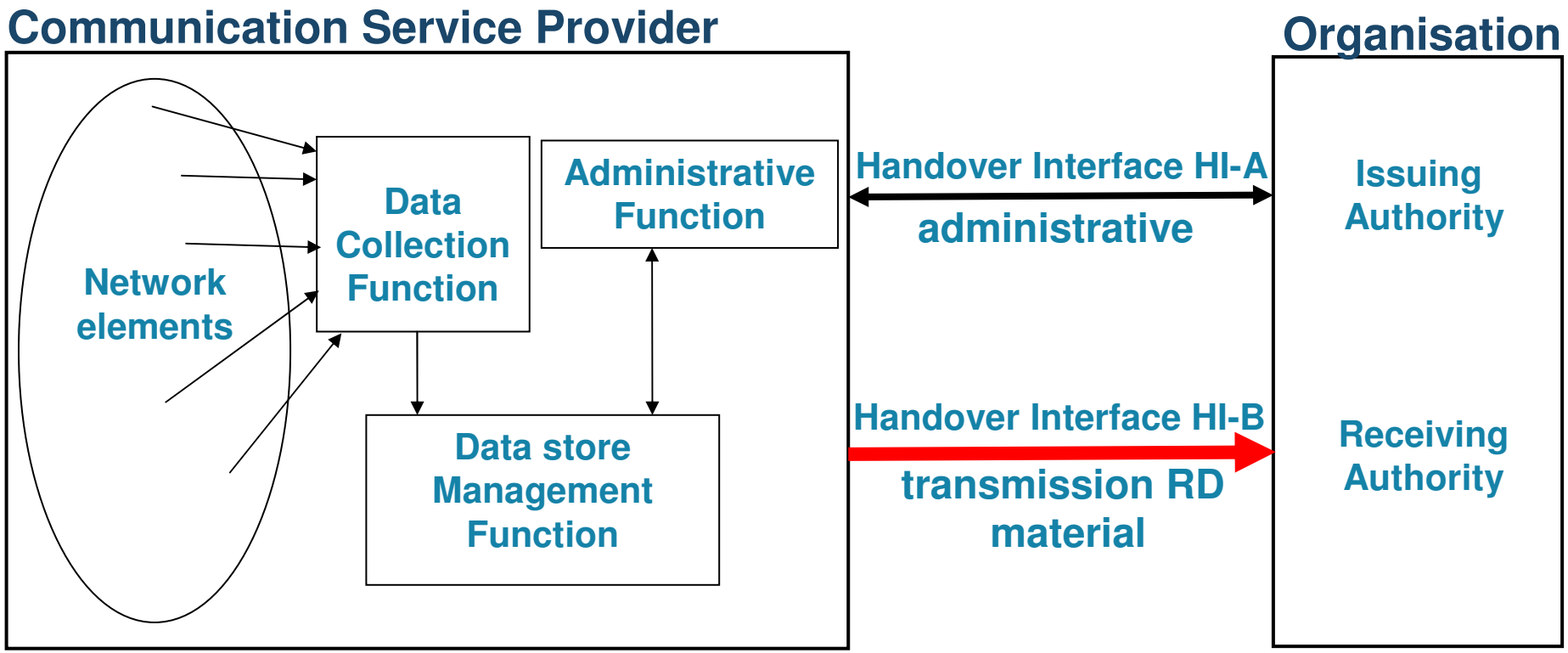
The Data Retention Puzzle



Why standardisation of RD handling

- Easier to define own storage and delivery mechanism
  - No need to define/invent complete own delivery / receiving system
  - National options are possible
- "Cheaper" products
  - Manufacturers need to develop one basic product
  - National options are additional
- Data Retention result is meeting international and national requirements
- RD Standards in ETSI are actively developed in good harmonization and are approved by all involved parties
- Common way for all involved parties
- Continuous increase in types of Retained Data
  - Use of the telecommunication
  - Number of different services used
  - Number of different access networks used

Functional Model



HI-A: various kinds of administrative, request and response information from/to the Issuing Authority and the responsible organization at the CSP for RD matters.

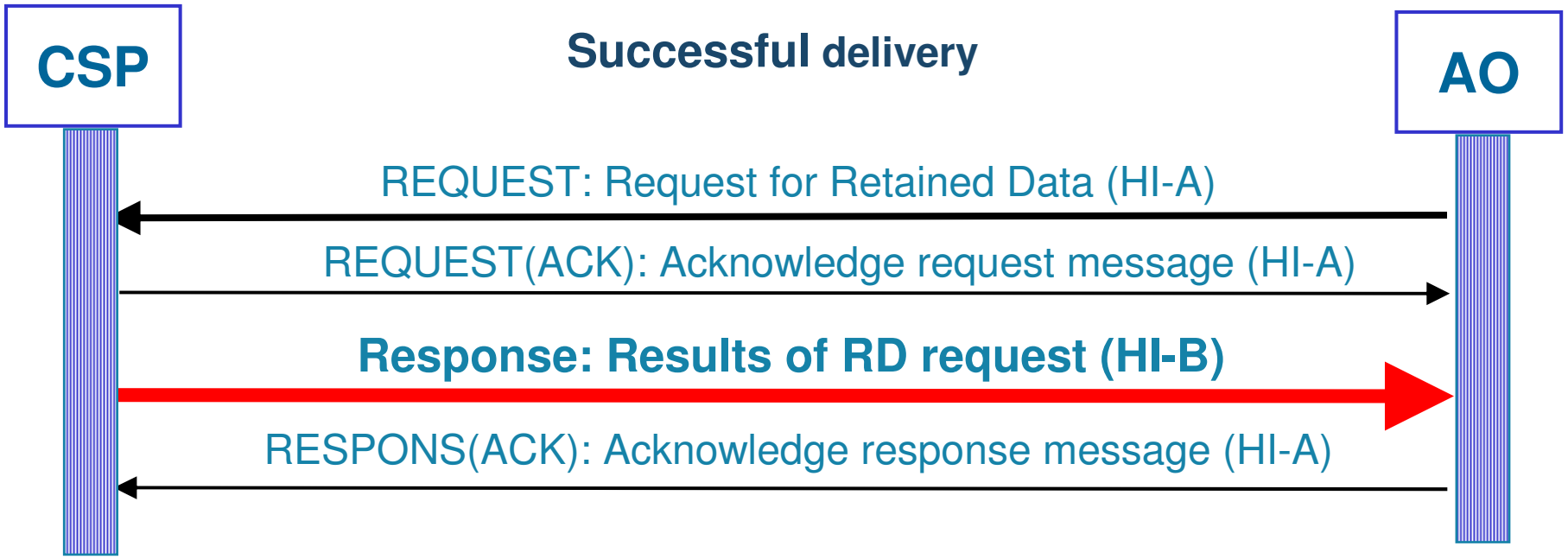
HI-B: retained data information from the CSP to the Receiving Authority

HI-A and HI-B may be crossing borders between countries:
subject to corresponding national law and/or international agreements.

Retained Data Specifications in ETSI/TC LI

- ***ETSI TS 102 656*** ***(v1.2.1)***
  Requirements of LEAs for handling Retained Data
  - guidance and requirements for the delivery and associated issues of retained data of telecommunications and subscribers
  - set of requirements relating to handover interfaces for retained traffic and subscriber data
  - requirements to support the implementation of Directive 2006/24/EC
  - freedom for national regulations, procedures and processes
- ***ETSI TS 102 657*** ***(v1.4.1)***
  Handover interface for the request and delivery of Retained Data
  - handover requirements and handover specification for the data that is identified in EU Directive 2006/24/EC on Retained Data and in national legislations as defined in TS 102 656
  - considers both the requesting of retained data and the delivery of the results
  - defines an electronic interface

Retained Data Handover Signalling principle



- **Data exchange techniques**
  - **"direct TCP" with BER encoding derived from the ASN.1**
  - **"HTTP" with XML encoding**
    - **on top of the standard TCP/IP stack**
    - **choice of technique is a national option**

Retained Data requests

- A request may only ask for data from **one service**
  - Telephony services
  - Network access services
  - Asynchronous message services
  - Synchronous multi-media services
- A request may only ask for data from **one category**
  - Subscriber data — e.g. subscriber ID, name, address, NRI
  - Usage data — e.g. call records
  - Equipment data
  - Network element data — e.g. location and identity GSM base station
  - Additional service usage — e.g. DSN
- A request shall list one or more request **criteria**
  - Equal To — a specified value for a given field
  - Range — a range for a given field (e.g. lower and upper bounds, using the lessThan or greaterThan operators)
  - Member of — a list of values for a given field

Examples of Requests (TS 102 657)

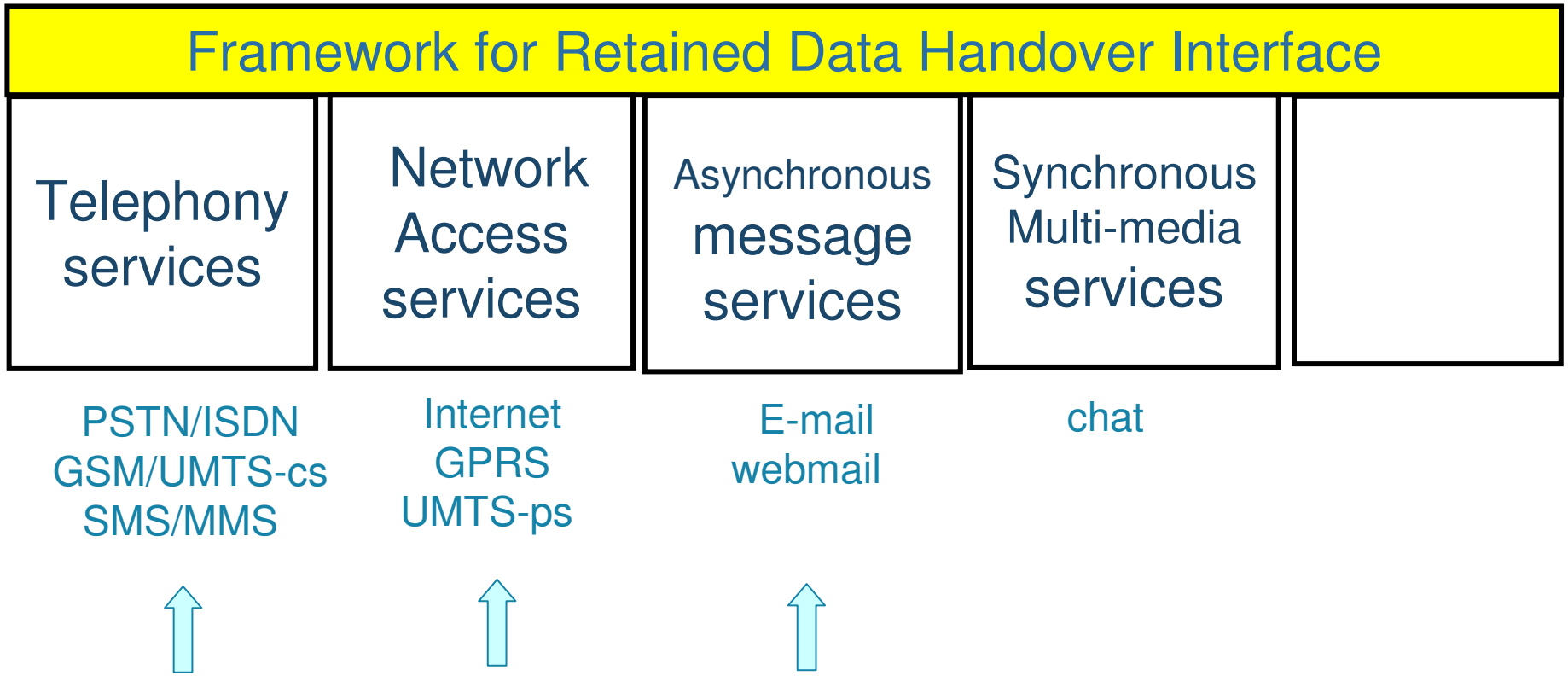
- Please provide data for **subscriptions** with telephone number 0123456789, which were started in the time span between 1 August 2009 and 15 September 2009

Request Parameter	Value
registeredNumber	Subscriber record for telephony service with matching phone number is returned
timeSpan	A range of times for the start of the subscription

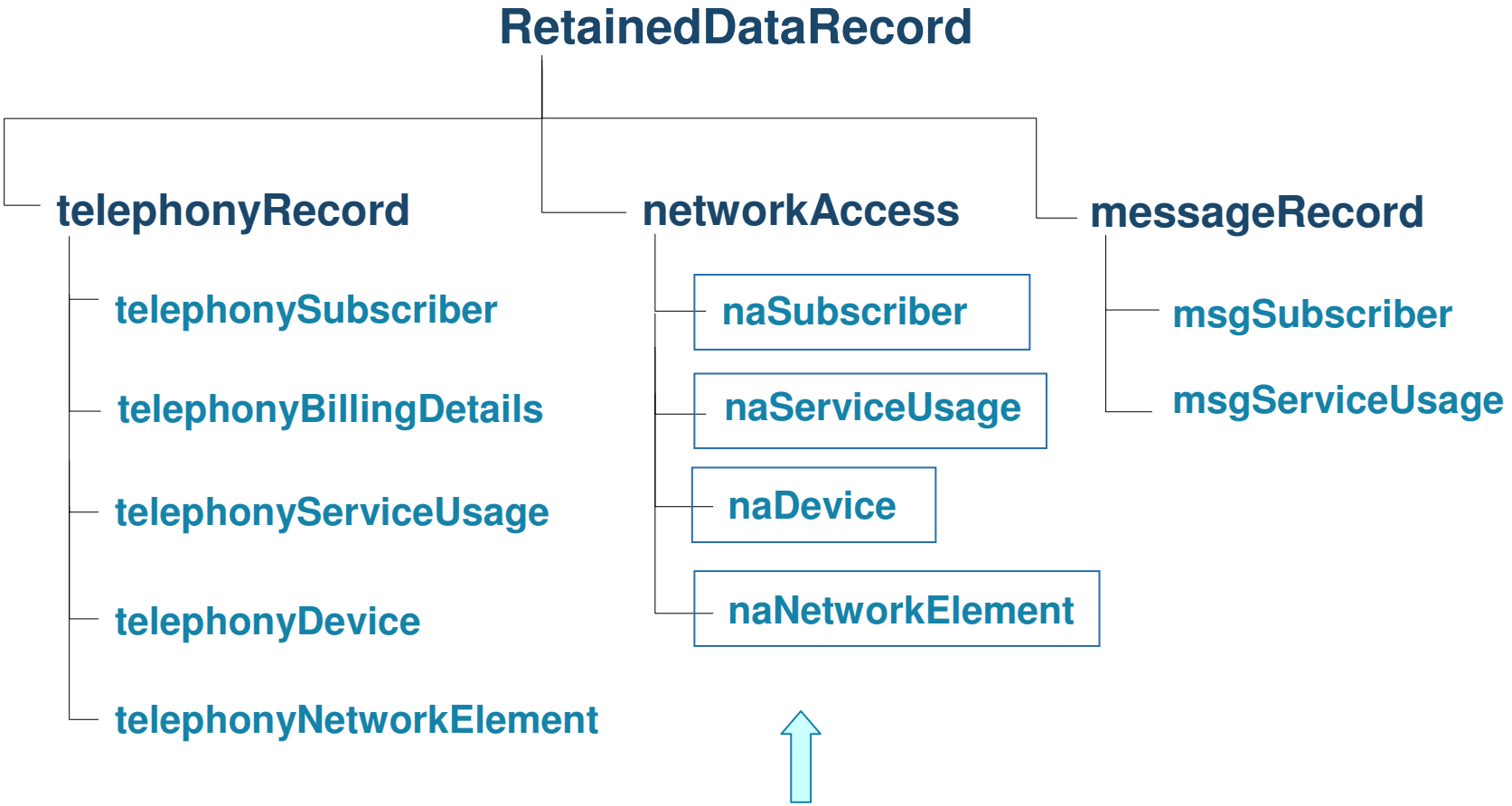
- Please provide service **usage** records for phone number 0123456789 for calls, which were initiated from that number between 5 September 2009 and 15 September 2009

Request Parameter	Value
partyNumber	Telephone number of interest in the call
partyRole	Role (originating or terminating) of the telephone number specified (can be omitted)
timeSpan	A range of times for the start of the call

Modular approach RDHI specification



Schematic representation of top level ASN.1



networkAccess: Subscriber

naSubscriber

- validity
- subscriberID
- naSubscriptions
  - NAServiceSubscription
    - validity
    - naServiceID
    - naProviderID
    - naAuthID
    - options
    - installationAddress
    - fixIpAddress
    - imsi
    - allocatedDeviceIDs
- allocatedDeviceIDs
- genericSubscriberInfo

GenericSubscriberInfo

- organizationInfo
  - name
  - contactDetails
  - nationalRegistration
- individualInfo
  - name
  - contactAddress
  - dateOfBirth
  - gender
  - identificationNumber
  - authenticationInfo

networkAccess: ServiceUsage, Device and NetworkElement

naServiceUsage
- naAccessTime
- naAuthID
- nwAccessType
- naStatus
- interval
- naDeviceId
- naNwElementID
- naAssignedAddress
- location
- dialUpInformation
- gprsInformation
- octetsUploaded
- octetsDownloaded

naDevice
- naDeviceId
- description
- location
- macAddress
- dslId
- imei

naNetworkElement
- validity
- naNwElementID
- naProviderID
- supportedAccessTypes
- location

National Implementation

- Definition of the set of elements to be retained
- Definition of the format of the requests
- Which standard to be used for the request and for transport of requested data

- Preparation of ETSI handover specification for national implementation
  - definition of the optional elements for national use
  - how to use specific elements
  - definition of specific national elements
  - transport mechanism to be used
  - security mechanisms

Activities in EC/Expert Group:

"The Platform on Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime"

Guidance Papers in relation to its application in the DR Directive

- Closer understanding of the term "Internet e-mail", "Webmail" and "Web Based Messaging"
- The obligation to retain E-mail logs – when must records of spam E-mails be retained?
- Closer understanding of the term "Transit Providers"
- Closer understanding of the term "third party networks and service providers"
- Closer understanding of the term "Internet Telephony"
- Closer understanding of the term "Centralised Data Storage"
- Closer understanding of the term "Data Security"
- Closer understanding of the term "Port Numbers"
- Overview of available standards for Data Retention

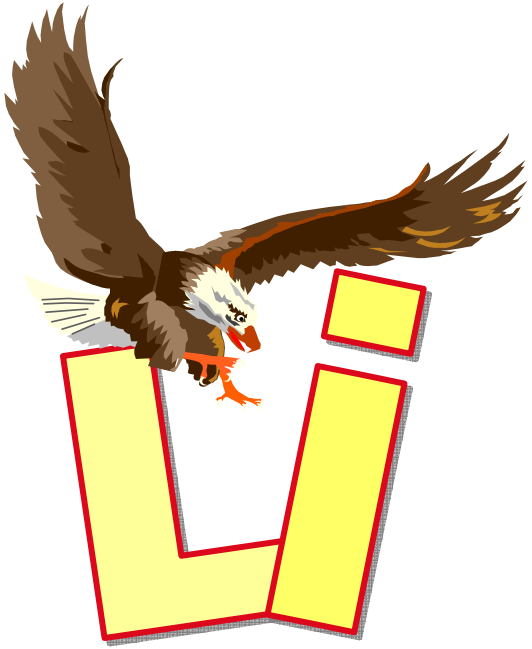
Intro on ETSI/TC LI .

- Created as stand-alone TC in October 2002
- Meetings
  - Three plenary meetings a year are organised (35-84 participants)
  - Dedicated Rapporteur's meetings can be organised on a specific issue (actual study item is "Dynamic Triggering")
- The meetings can be attended by ETSI members
  - Non-ETSI members can participate by invitation of the chairman
  - Next meeting: ETSI/TC LI#23, 9-11 February 2010 in Rome
- Dedicated TC LI e-mail server and document server
  - Open to all (registered) ETSI members
- Producing reports and specifications
  - On Lawful Interception and Retained Data
  - Mainly on the Handover Interface
- Promoting globally ETSI Lawful Interception and Data Retention standards amongst operators and national bodies

Participation in ETSI/TC LI

- Law Enforcement Agencies / Governments organisations / Research organisations
  - NL, UK, DE, AS, S, GR, ES, FR, FIN, CH, RU, UA, IT, NO, CY, HU
  - AU, CA, USA, ID, KR
- Communication Service Providers
  - Vodafone, KPN (NL), BT (UK), DT (DE), TeliaSonera (S), Inmarsat, RIM Telenor, T-Mobile, Telecom Italia, Swisscom, Wind, UPC, TDC (DK) Telstra (AU), NBIP (NL)
- Manufacturers (switch / mediation / LEA equipment)
  - Ericsson, Siemens, Nokia Siemens Networks, Trovicor, Alcatel-Lucent Pine Digital Security, Group 2000, Aqsacom, Cisco, GTEN, DARS Utimaco Safeware, Verint, NICE Systems, Detica, Thales, Iskratel, HP ATIS Systems, SS8, Spectronic Systems, Nortel, AREA, ETI, IPS Suntech, VeriSign, ZTE

Manufacturers may be active in more areas

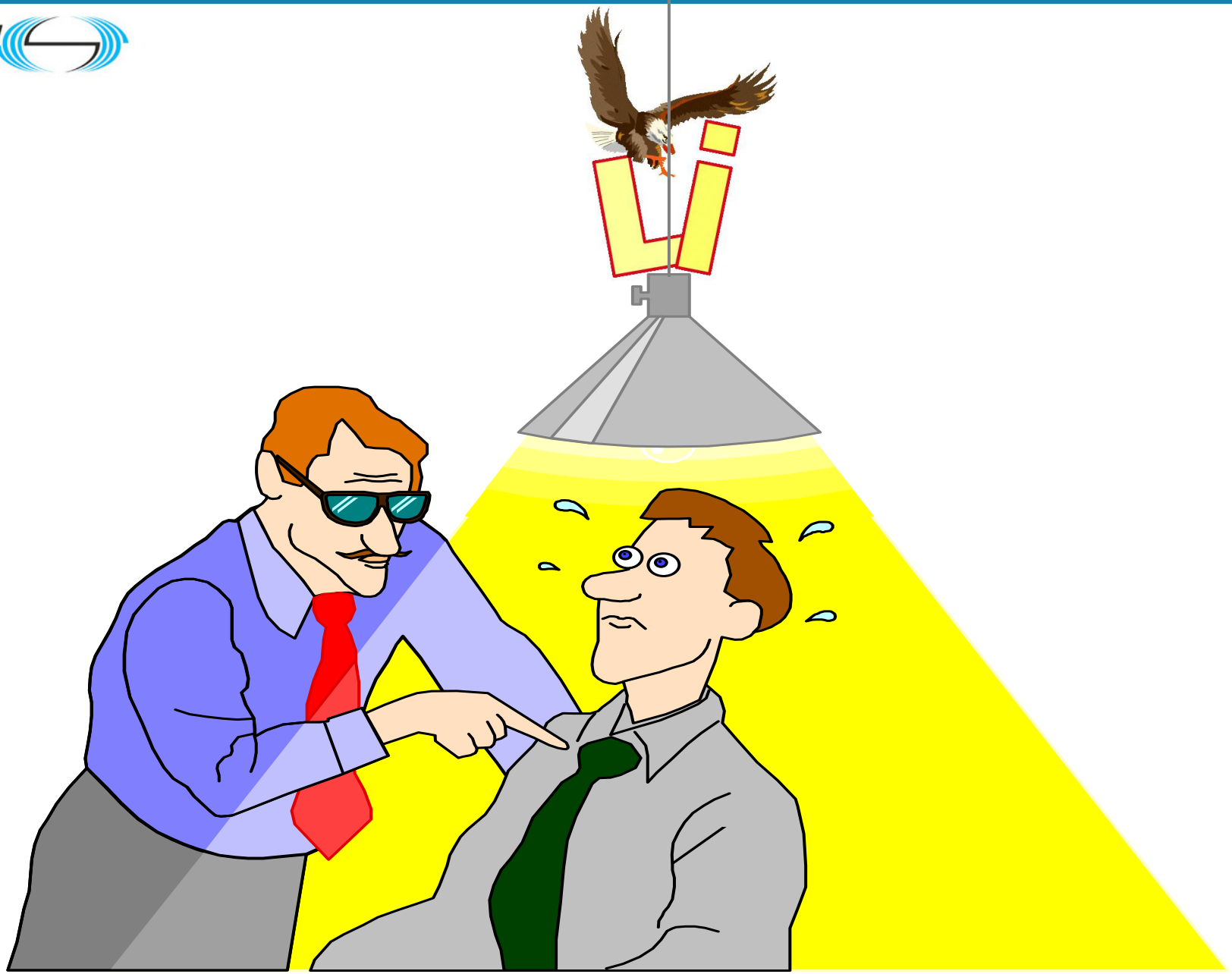


More details on ETSI/TC LI can be found on:

http://portal.etsi.org/li/Summary.asp

Chairman TC LI: Peter@DataRetention.eu
Peter@Lawfulinterception.com

All publications freely available! Downloadable from ETSI Website
http://pda.etsi.org/pda/queryform.asp



Ministerie van Economische Zaken

Ministerie van
Economische Zaken

BEWAARPLICHT TELECOMMUNICATIE-GEGEVENS

14 oktober 2009