A Corporate Perspective on Data Protection

SPEAKERS:

Steve Mutkoski, *Microsoft*

«Regulatory Trends in Healthcare Data»

Richard Kemp, *Kemp IT Law*

«Secondary Use of Personal Data»

Martin Johansson, *Advokatfirman Vinge KB*
Stefan Backman, *Tele2*

«Joined cases C-203 / 15 and C-698 / 15, Tele2 Sverige and Watson and Others»

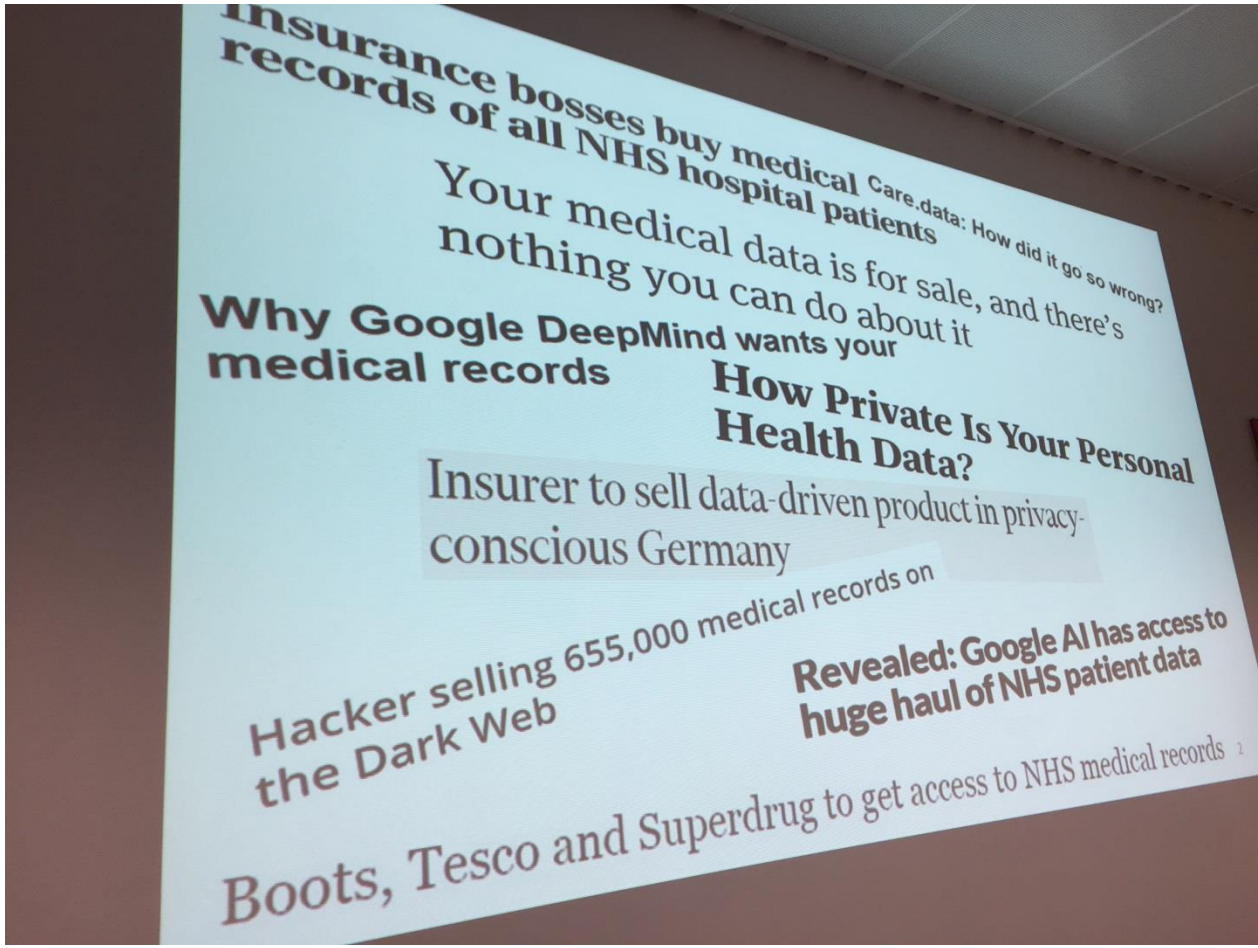
MODERATOR: Dr. András Gurovits, *Niederer Kraft & Frey Ltd*

Healthcare and Cloud Computing: Regulatory Trends

Steve Mutkoski
Government Affairs Director
Microsoft Healthcare Industry Group

Health Data and Headlines

- Policy Imperatives– Urgent need to leverage new technologies like cloud and mobile to lower cost, improve care outcomes and increase access to care.
- A Balancing Act– Keep sensitive health information secure and ensure pragmatic restrictions on access and use.
- Tremendous opportunity for positive outcomes, potential to make mistakes and to lose patient or public trust



Record Storage Requirements

Belgium

*"each patient must have a patient record . . . kept **in** the hospital"*

*"each patient must have a patient record . . . kept **by** the hospital"*

Amendments to Article 20 of the Coordinated Law of 10 July 2008 in hospitals and other care facilities, published on April 30, 2014 removed on premises requirement and replaced it with a stewardship concept.

Poland

"treatment record is [to be] stored in the organizational unit which provides the healthcare service for the entire period of the patient's treatment"

"Internal records are stored by the entity which produced them"

A revised version of a 2010 regulation on the handling and storage of medical records that went into effect in November 2015 removed the language requiring on premises storage.

Physician-Patient Confidentiality

Germany

Sec. 203 German Criminal Code (strafgesetzbuch), ¶ 1:

(1) Whosoever unlawfully discloses a secret of another, in particular, a secret which belongs to the sphere of personal privacy or a business or trade secret, which was confided to or otherwise made known to him in his capacity as a

1. physician, dentist, veterinarian, pharmacist or member of another healthcare profession which requires state-regulated education for engaging in the profession or to use the professional title; . . .

shall be liable to imprisonment not exceeding one year or a fine.

In June 2017, the German parliament amended section 203 at the Penal Code to allow for use of cloud computing services where the security and privacy of such professional secrets could be ensured (through contract terms and technological measures). Amendments recognized "mitwirkenden Personen" (or "participating persons") and not just employees can preserve secrets.

Poland

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Speech GIODO of 23 August 2011 to the Minister of Health to undertake legislative work aimed at introducing legal basis for commissioning of computerized processing of personal data by data administrators processing personal data of patients in connection with the provision of health services to other specialized entities in this field (called outsourcing), along with the reply and further correspondence.

In Poland, HCOs operated under the cloud of a letter from the Inspector General for Personal Data Protection to the Minister of Health which stated that healthcare providers could not "outsource" data processing due to physician-patient confidentiality concerns. 2015 amendments to the Act on Patients' Rights and the Patients' Ombudsman authorized the use of cloud computing services, "provided that data protection is ensured and that the [healthcare providing] entity retains the right to control whether the processing medical data takes place in compliance with the contract" and that the outsourcer must be "obliged to keep confidential all information regarding the patient which it obtained as a result of the execution of the contract."

Conflicting Policies

UK data protection authority (ICO): *"There are **no restrictions on the transfer of personal data to EEA countries.**"*

Department of Health, 2013: "*there is **no Department for Health policy stating that patient information must be held in England**"*

NHS 'Connecting for Health' agency (now HSCIC), 2009: "*[i]n respect of systems and applications connected to [HSCIC] systems and applications **Patient Identifiable Data should not be recorded outside of the England boundary in any format for any reason** without the prior explicit written permission of [HSCIC].*"

Patient Consent

Most laws presume consent for treatment, billing, operations

HIPAA Privacy Rule, GDPR Article 9(2)(h)

Should patients be required to consent to use of certain types of technology for such primary or direct care uses?

Un dispositif prévu par la loi

Les modalités d'hébergement de données de santé à caractère personnel sont encadrées par l'article L.1111-8 du code de la santé publique :

- Toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social ou médico-social **pour le compte d'un tiers**, doit être agréée à cet effet ;
- L'hébergement exige une information claire et préalable de la personne concernée par les données de santé hébergées et une possibilité pour celle-ci de s'y opposer pour motif légitime.

The hosting of personal health data is governed by Article L.1111-8 of the Public Health Code:

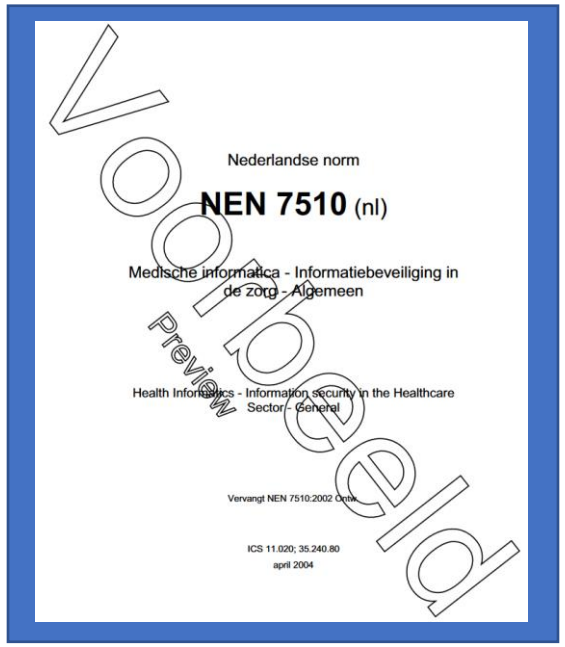
■ Any natural or legal person who hosts personal health data collected from time to time prevention, diagnosis, care or social or medico-social monitoring on behalf of a third party must be approved for that purpose;

■ ***Hosting requires clear and preliminary information from the person concerned by the hosted health data and a possibility for it to oppose it for legitimate reasons.***

Multiple Regulations - Germany

Federal	• Data Protection Law governing federal hospitals
State	• Data Protection Laws in all 16 states governing regional hospitals
Religious	• Church-affiliated hospitals can set their own data protection rules
Other	• Additional rules in the Federal Cybersecurity Act, Drug Act, Medical Devices Act, Criminal Code, Social Security Codes, State Hospital & Health Data Acts

Baseline Security Requirements



Draws heavily from ISO 27001

Agrément des hébergeurs de données de santé : publication du référentiel de certification pour concertation

SERVICES | 16 SEPT. 2016

Law n ° 2016-41 of January 26, 2016 of modernizing our health system provides for the replacement of the approval procedure by a technical conformity assessment by a certifying body accredited by the French accreditation committee COFRAC. The objectives of the new certification procedure are to put the process in a well-known industrial procedure (notably the ISO 27001 certification) and to increase the reliability of the control of the requirements by on-site audits. As a result of joint work with the Delegation to the Health Information Systems Strategy (DSSIS) and stakeholders, this certification framework for health data hosts is published today for public consultation.

Streamlining Regulatory Processes

French law requires entity hosting personal health data on behalf of HCO must be approved:

- Only granted after reasoned opinions from the Accreditation Committee of Hosts (CAH) and the Data Protection Authority (the "CNIL") with 12-18 month process not unrealistic.
- ASIP's own estimate, as much as 50% of health data is likely hosted without such prior approval, possibly due to the cumbersome and bureaucratic process.
- Even new "certification" process looks to create a bottleneck.

New Zealand Ministry of Health

- Prior system required centralized approval
- Effective April 2017 each healthcare entity must undertake its own risk assessment, as per guidelines issued by the Government CIO's Office

US Health Insurance Portability and Accountability Act. Since April 2003, OCR has:

- received over 163,277 HIPAA complaints and resolved ninety-eight percent of the complaint cases (159,633).
- investigated and resolved over 25,373 cases by requiring changes in privacy practices and corrective actions
- settled 52 such cases resulting in a total dollar amount of $72,929,182.00

Key Lessons:

- Centralized approval can be a huge bottleneck
- Multiple agency approval multiplies the delays
- Consider self-assessment against clear requirements
- Use audit and sanction to ensure compliance

General Data Protection Regulation

- Things that stay similar/the same:
  - Art 9: “data concerning health” is a special category of personal information. “Member States may maintain or introduce further conditions, including limitations, with regard to the processing of [such data]”
  - Art 89: Safeguards and derogations for research “Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards”
- Things that change:
  - New Data Subject Rights (Rectification and erasure, Data Portability, etc)
  - Substantial fines, including for Processors
- Challenges:
  - HCOs are often federated organizations with many small affiliates and loosely grouped
  - IT and data governance are often left to affiliates

Henrietta Lacks

- 1951: Henrietta, a poor tobacco farmer from southern Virginia died from cervical cancer
- 1976: Her family learned that a biopsy of her cancerous tumor had been used for the last 2 decades to propagate cells for lab research
- Today: Estimates are that 1 in 5 people who lived since her death have benefited from a therapy developed as a result of these cell cultures
- Prior to the “HeLa” cell line, researchers were unable to grow human cells in a lab. Her cells were taken and used without consent, initially with no understanding that they would reproduce and grow on their own. In 1951, there was no existing notion of consent.

ITECHLAW 2017 European Conference

Secondary Use of Personal Data – Recent UK Developments

Richard Kemp

Stockholm, October 20, 2017

KEMP IT LAW

kempitlaw.com

framing the secondary processing debate

GDPR Art 5(1)(b)

- generally, research and other secondary processing need their own lawful processing basis
  - personal data must be collected for [primary] specified, explicit and legitimate purposes
  - not to be further [secondarily] processed incompatibly with those primary purposes;

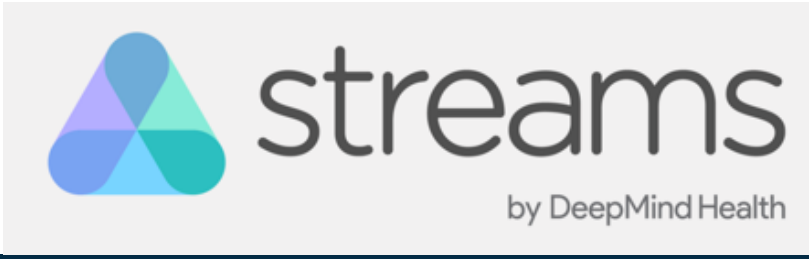
- but Member States can alter that by setting out appropriate safeguards under Art 89(1)
  - further processing for ‘archiving purposes in the public interest, scientific or historical research purposes or statistical purposes’ ‘subject to appropriate safeguards’ is OK;
  - data controllers could do research without further consent where Member States had set out ‘appropriate safeguards’

DeepMind/Royal Free – a live example from the UK

- Jan 2014: Google acquires London-based AI developer DeepMind Technologies
- Sept 2015:
  - Royal Free is developing ‘Streams’, a kidney injury detection, diagnosis & prevention app
  - Information Sharing Agreement (ISA) signed for DeepMind to process personal data of 1.6m Royal Free patients for clinical safety testing of ‘Streams’
  - PD is sent not subject to pseudonymisation as Royal Frees believe the data is being processed with ‘implied patient consent’ for the purpose of ‘direct patient care’

DeepMind/Royal Free – a live example from the UK

- Nov 2015: data streaming starts
- April 2016: Sept 2015 ISA obtained via FOI request and published
- May 2016: ICO opens investigation
- Feb 2017: Streams mobile app goes live
- July 2017: ICO publishes findings and the undertakings it is seeking from Royal Free



DeepMind/Royal Free – ICO's 3 July 2017 decision

- **Principle 1: fair and lawful processing**
  - *The processing of patient records by DeepMind significantly differs from what data subjects might reasonably have expected to happen to their data when presenting at the Royal Free for treatment."*
  - The secondary processing did not constitute 'direct patient care'
  - There was no implied consent, and DeepMind's processing was in breach of the duty of confidence that Royal Free owed its patients

- **Principle 3: adequate, relevant and not excessive**
  - *it was not "necessary and proportionate to process 1.6m patient records to test the app's clinical safety."*

ico.
Information Commissioner's Office

DeepMind/Royal Free – ICO's 3 July 2017 decision

- **Principle 6: compliance with data subjects' rights**
  - *"if patients did not know that their information would be used in this way they could not take steps to object"*

- **Principle 7 – appropriate technical and organisational measures**
  - *Agreement "did not contain enough detail to ensure that only the minimal possible data would be accessible to DeepMind."*
  - *"… processing of such a large volume of records containing sensitive health data was not subject to a full privacy impac assessment ahead of the project"*

ico.
Information Commissioner's Office

DeepMind - the UK National Data Guardian's view

"Royal Free shared the data on the basis of 'implied consent for direct care'. I came to the view that they had not used an appropriate legal basis for data sharing. This legal basis cannot be used to develop or test new technology, even if the intended end result is to use that technology to provide care."

We can earn public support for the use of data in innovation, by "adhering to explicit and transparent principles of good practice" to "reassure patients and those treating them that confidentiality is safeguarded". The public rightly expects nothing less."

National Data Guardian

DeepMind case points up policy aims in tension

- where the government is the main payer – like the UK for the NHS - why shouldn't it be allowed to use aggregated patient data to improve care for others?
- who wouldn't want to see primary care providers with a tool to identify patients at risk of kidney damage?
- any AI tool (in any industry) implies huge amounts of data to train the machine learning model/algorithm

DeepMind case points up policy aims in tension

- what use can the care provider as data controller make of the data under GDPR?
  - is patient consent always needed?
  - when is it not needed?
  - when obtained, what use is consented to/permitted?
- who (including commercial entities) can use/derive benefit from that data?
  - specialist commercial entities can do this better than the care provider
  - In the USA, AI providers are working with care providers to build algorithms based on large patient records datasets
- how do we rebuild trust in AI-based healthcare research in the UK?

way forward (1): Royal Free undertakings compliance

Royal Free has agreed to give five undertakings requested by ICO:

[1] within 2 months, to carry out a PIA

within 1 month of the PIA to show how [2] the 'fair & lawful processing' and [3] the Schedule 3 sensitive information processing requirements are met, and [4] it will comply with its duty of confidence to patients

[5] within 3 months of the undertaking to commission a compliance audit

Royal Free website:

"We have signed up to deliver all of and have started working on the undertakings – including delivering a third privacy impact assessment of our work with DeepMind, continuing to be open and transparent about how we use patient information and conducting a third party audit of our current processing arrangements with DeepMind."

- watch this space

way forward (2): ICO paper of 04.09.17

- v1.0 ‘Big Data and Data Protection’ paper published in 2014
- v2.0 published April 2017
- v2.2 published on 4 September 2017

six key recommendations:

1. does the big data analytics need personal data to be processed?
2. provide meaningful icons, notifications and privacy notices
3. embed a PIA framework into big data processing activities
4. implement a privacy by design approach
5. develop ethical principles to reinforce data protection principles
6. develop auditable machine learning algorithms

way forward (3): Art 89(1) & what Member States can do

In the UK, the Wellcome Trust has done significant work in this area

- *"Member States should ensure their legal framework is sufficient to implement Article 89 and facilitate scientific research"*
- *"Passing specific legislation is likely to provide the clearest and most certain framework for researchers"*
- *"We encourage Member States to work together to promote compatibility between national approaches where possible to facilitate cross-border research"*

(Wellcome Trust Data Protection Regulation Site)

thank you

Richard Kemp

richard.kemp@kempitlaw.com
+44 20 3011 1670

KEMP IT LAW

kempitlaw.com

VINGE

JOINED CASES C-203/15 AND C-698/15, TELE2 SVERIGE AND WATSON AND OTHERS

- Data retention by providers of electronic communications services

iTech Law European Conference, Stockholm 2017

Stefan Backman, Tele2;
Martin Johansson, Advokatfirman Vinge

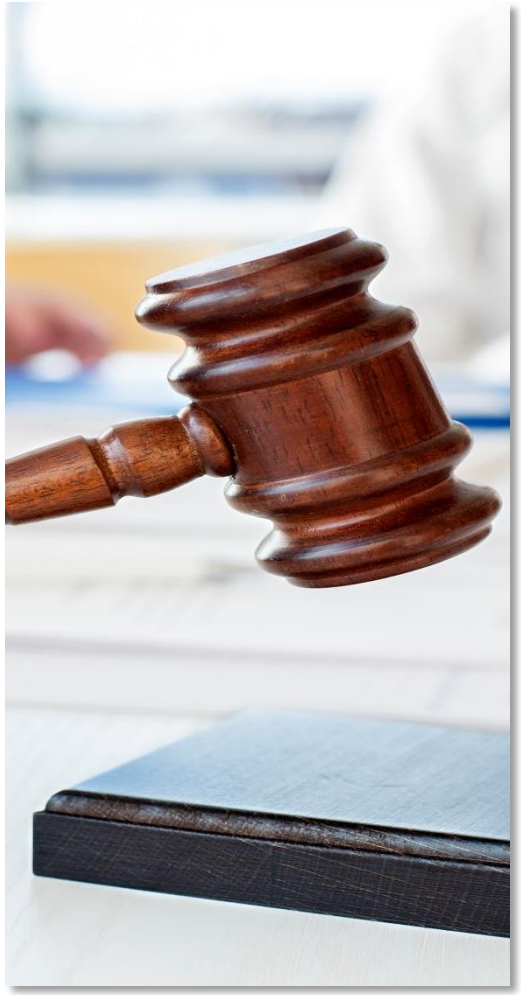
Background to the proceedings in Luxembourg

1. Data Retention Directive 2006/24 implemented in Swedish legislation:
   - Providers of publicly available electronic communications services or of public communications networks subject to a general obligation to retain all traffic and location data generated or processed by them; and
   - Under certain conditions, access to this data to be granted to national authorities.
2. Data Retention Directive 2006/24 declared invalid by the CJEU in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, 9 April 2014:
   - Data retention requirements disproportionately interfered with fundamental rights protected by the EU Charter of Fundamental Rights.
3. Tele2 informs the Swedish Post and Telecom Authority (“PTS”) that it will no longer retain data and that intends to erase data previously recorded.
4. Public inquiry ordered by the Government. Report concludes that the Swedish legislation does not violate EU law.

Background to the proceedings in Luxembourg cont.

5. PTS orders Tele2 to commence the retention of data. Tele 2 takes legal action against the order.
   - Tele 2 looses in the Administrative court of first instance. Appeal.
   - Administrative Court of Appeal in Stockholm stays the proceedings and makes a reference for a preliminary ruling to the CJEU.
6. The Administrative Court of Appeal seeks clarity on the following questions:
   - Is a general and indiscriminate obligation on providers of electronic communications services to retain traffic and location data in order to fight crime compatible with EU law?
   - What are the relevant EU law requirements governing access and protection of retained data?
7. Reference from the Swedish Court is joined with a preliminary ruling reference from the Court of Appeal in England where similar issues have arisen.
8. 15 EU Member State governments submitted observations to the CJEU:
   - All opposing limitations on the possibilities for the Member States to impose data retention requirements on telecommunication companies.
9. CJEU Grand Chamber – 15 judges – judgment 21 December 2016.

The CJEU's judgment - Retention of data



- National legislation on retention of data and access to that data by national authorities falls within the scope of Directive 2002/58 and it is therefore within the parameters of EU law.
- Data retained according to the Swedish legislation allows very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained:
  - Particularly serious interference with the rights under Articles 7 and 8 of the Charter (rights to privacy and to protection of personal data) + has effects on the exercise of the rights under Article 11 of the Charter (right to freedom of expression).
- Such serious Interference with these fundamental rights can only be justified on the basis of an objective of fighting <u>serious</u> crime.

The CJEU's judgment cont. - Retention of data

- Such an objective of general interest not itself enough to justify a general and indiscriminate retention of all traffic and location data. No requirement that a relationship between the data which must be retained and a threat to public security.
- Therefore exceeds the limits of what is *strictly necessary* and could not be justified within a democratic society.
- However, Member States may, as a preventive measure, impose *targeted* data retention, for purpose of fighting serious crime, if limited with regard to the categories of data, the means of communication, the persons and the retention period, to what is strictly necessary.
- There must be clear and precise rules governing scope of application and imposing minimum safeguards.
- The retention must meet objective criteria establishing connection between the data and the objective pursued; The legislation must be based on objective evidence.

The CJEU's judgment cont.
- Access by competent national authorities to retained data

- Must correspond to one of objectives set out in Article 15(1) of the Directive 2002/58 – safeguard of national and public security, defence and the fight against serious crime.

- Requires legally binding, clear and precise national rules, laying down the substantive and procedural conditions governing access, based on objective criteria, under which:
  - Access can only be granted to the data of *individuals suspected* of planning, committing or having committed a serious crime or of being *implicated* in one way or another in such a crime. Exception: threat of terrorist activities – other persons if in a specific case would make effective contribution.
  - *Prior review* carried out either by a court or by an independent administrative body.
  - Competent national authorities must *notify* the persons affected as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities.

- *Providers of electronic communications services* must ensure a particularly high level of protection of retained data against risks of misuse and against any unlawful access to that data:
  - Data has to be retained *within* the European Union.
  - Irreversible destruction of the data at the end of the data retention period.

- Review by independent authority of compliance with the level of protection ensured under EU law.

Reactions to the judgment

- The judgment of the CJEU did not come as a complete surprise: *Digital Rights Ireland*; *Schrems*
- The most surprising part of the judgment: rejection of the possibility for the Member States to maintain a national general data retention obligation.
- Question: what balance fighting crime and terrorism vs. personal freedoms (privacy)?

Reactions to the judgment cont.

Positive reactions:

- The right to private life and to the protection of personal data require strong safeguards in an age of digitalisation (Big data, government surveillance):
  - Retention of personal data only when strictly necessary.
  - Access to retained data only for defined purposes and under adequate procedural safeguards.
- Limits risk of erroneous correlations and suppositions that may lead to discrimination.
- Avoid “chilling effect” – limitation of one’s own freedoms because of feeling watched.

Negative reactions:

- Data retention less effective as crime reduction measure - Suspects often not known in advance.
- Communication of data could be valuable to law enforcement bodies also in investigations which do not concern serious crime (e.g. missing persons).
- The CJEU did not consider the important resulting practical issues of limiting the data retention.

Some reactions to the judgment in the United Kingdom

- A radical, but not surprising, decision, that will be of serious concern to law enforcement in the UK and other Member States.
- The judgment possibly enlarges the scope of EU law.
- Mixed reviews – the judgment was much needed/it is a disaster.
- The judgment will trigger debates in the Parliament, e.g. concerning:
  - boundaries between general and targeted data, and
  - what objective test should be used.
- Some sections in the judgment are vague, giving the national courts wiggle room.
- United Kingdom will be bound by the judgment up until it has left the EU, but may well play a central role also after Brexit.

The present situation in the EU

- Practically no Member States are currently complying with the requirements set out in the judgment.
- A legal framework with adequate protection must be implemented in nearly all Member States.

Concluding remarks

- The CJEU's judgment is clearly not the last word. The judgment clarified certain points, but opened others. The rules set out therein will need to be refined.

- The judgment is likely to bring about further discussions concerning surveillance capabilities – increased critical review of all the arguments and evidence that speaks for or against data retention.

WHAT HAS HAPPENED IN SWEDEN AFTER THE CJEU JUDGEMENT?

VINGE

Actions in Sweden following the CJEU judgement

- Administrative Court of Appeal revokes PTS order against Tele2 (other EU Member States have followed the same path)
- Tele2 (and all other Swedish operators) stops retaining data on behalf of authorities.
- Big public debate regarding need for personal integrity vs effective crime fighting. Police and prosecutors alarming in the debate.
- New public inquiry ordered by the Government (aim is new more balanced data retention legislation).
- Tele2 engages in dialogue regarding interim measures with police and prosecutors.
- Results of public inquiry to be published mid October.
- New legislation expected to enter into force during 2018.
- New appeals?

VINGE

STOCKHOLM
GOTHENBURG
MALMO
HELSINGBORG
BRUSSELS

www.vinge.se

Discussion