CloudWatch

Think Cloud Services for Government, Business & Research

Become legally compliant using CloudWATCH2 Legal Guides

Nicola Franchetto, ICT Legal Consulting & Partner, CloudWATCH2

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

AGENDA

- Introduction to the GDPR
- CloudWATCH 2 Legal Guides
- GDPR: Key definitions, substantive principles, game changers and methodology
- Q&A

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Introduction to the GDPR

2012

- *Start of reform process aiming to align data protection laws of the EU's 28 Member States, and update rules for the digital age*

April 2016

- *GDPR is enacted after years of difficult negotiations*

May 4 2016

- Text published in the OJEU - enters into force 20 days after publication

May 25 2018

- *GDPR applies throughout the EU after 2-year transition period*

Current legal framework based on Directive 95/46/EC inconsistent patchwork of national laws.

GDPR objectives: high level of protection (maintains data protection principles), modernization, harmonization, more effective implementation

European Commission | ©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Applicable Law

- **Broader territorial reach than the current regime**
  - Test 1: GDPR applies where processing takes place "in the context of the activities of an establishment of a controller <u>or processor</u> in the EU"
  - Test 2: GDPR applies to controllers outside the EU when processing activities relate to:
    - offering goods or services to data subjects in the EU
    - monitoring the behavior of data subjects in the EU
  - No longer apply "making use of equipment" test

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

CloudWATCH 2 Legal Guides

- **Pre-contractual phase**
- Jurisdiction & Applicable law
- Privacy Roles.
- Amendments to the contract
- Data location and transfers of data
- Processing of personal data by sub-contractors
- Data subjects' rights (or "Intervenability")
- Lock-in and Interoperability
- Service Level Agreements ("SLAs")
- Termination of the contract
- Privacy Level Agreements ("PLAs")

European Commission | ©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

GDPR: Key definitions

European Commission | ©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Key definitions (i)

- Controller - retained
  - The natural or legal person, public authority, agency or other body which, alone or jointly with others, **determine the purposes and means** of the processing of personal data.
- Processor- retained
  - A natural or legal person, public authority, agency or other body which processes personal data **on behalf of the controller**.
- Consent - amended
  - Any freely given, specific, informed and **unambiguous** indication of the data subject's wishes by which he or she, **by a statement or by a clear affirmative action**, signifies agreement to the processing of personal data relating to him or her.
- Main establishment – new
  - As regards a controller with establishments in more than one Member State, **the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment**.

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Key definitions (ii)

- Personal Data – retained (but mind the EU case law)
  - Any information relating to an identified or identifiable natural person ('data subject').
- Special – i.e., sensitive – Data - amended
  - Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and **the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person**, data concerning health or data concerning a natural person's sex life **or sexual orientation**.
- Pseudonymization - new
  - The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is not subject to technical and organisation measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Principles

European Commission | ©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Substantive Principles (i)

- **Lawfulness, fairness, and transparency**
- **Purpose limitation**
  - Incompatible further processing still prohibited
  - Criteria for assessing compatibility identified
  - Further non-consensual uses allowed in certain cases
    - where required by law; or
    - for scientific or historical research or statistical purposes
- **Data minimization**
- **Accuracy**
  - Including erasure and rectification “without delay”
- **Storage limitation**

Substantive Principles (ii)

- **Lawfulness of processing**
  - **Legitimate interests**
    - still a valid legal basis to process non-sensitive data
    - balanced against the interests and fundamental rights and freedoms of the individual – extra protection for children
    - reasonable expectations of the individual
  - **Consent**
    - specific and informed
    - unambiguous
      - statement or clear affirmative action
    - freely given – not the case where:
      - imbalance between the controller and the data subject
      - consent for non-essential processing is a precondition to entering into a contract
    - special rules relating to children in the context of information society services
  - **Other available grounds for lawfulness**

GDPR: Game changers

European Commission | ©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

GDPR: game changers

- Principle of Accountability (Art. 24 GDPR)
- Data subjects’ rights
- Enforcement, Sanctions and remedies

Accountability

European Commission
©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Accountability (i)

- **Responsibility of controllers**
  - To ensure and **to be able to demonstrate compliance** of data processing with the GDPR
    - may include appropriate data protection policies, approved codes of conduct or certification mechanisms

- **Data protection by design and by default**
  - Controllers to put in place measures to effectively implement data protection principles and to integrate necessary safeguards to comply with the GDPR and to protect data subjects' rights
    - *e.g.*, pseudonymization and data minimization
  - Controllers to implement privacy settings so that only minimal necessary personal data are processed
    - *e.g.*, personal data are not made public by default

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Accountability (ii)

- **Data protection officer ("DPO")**
  - Potentially required for controllers *and* processors
  - Must designate a DPO where core activities involve monitoring data subjects or processing special categories of data "on a large scale"
    - EU law or laws of Member States may provide for other situations where DPOs must be appointed
    - groups of undertakings may appoint a single DPO
  - Significant powers and independence of DPOs

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Accountability (iii)

- **Data protection impact assessment ("DPIA")** of envisaged processing operations *prior* to the processing
  - Mandatory for controllers where processing is likely to result in "high risks" for the rights and freedoms of individuals, in particular:
    - systematic and extensive evaluation of personal aspects based on automated processing and on which decisions with legal effects or similar significant effects on the individuals are based
    - processing on a large scale of special categories of data
    - systematic monitoring of a publicly accessible area on a large scale
  - Supervisory authorities ("SAs") to establish a list of processing for which a DPIA is (not) required
  - Prior consultation of SA where the DPIA indicates high risks

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Accountability (iv)

- **Data security**
  - Enhanced obligations both for controllers and processors in comparison to the current regime
  - List of possible types of security measures

- **Data breach notification**
  - <u>Controllers</u> to notify the *competent SA* "without undue delay" and, where feasible, no later than 72 hours after becoming aware
    - unless data breach is unlikely to result in a risk for rights and freedoms of individuals
  - <u>Processors</u> to notify *controllers* without undue delay
  - <u>Controllers</u> to communicate personal data breach to *data subjects* if likely to result in a "high risk" for the rights and freedoms of individuals, subject to exceptions (*e.g.,* encryption)
  - Form and content requirements
  - Controllers to document data breaches and to provide to SA

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Data Subject Rights

European Commission | ©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Data subjects' rights

- Right to access (Art. 15 GDPR)
- Right to rectify (Art. 16 GDPR)
- Right to restrict (Art. 18 GDPR)
- Right to object (Art. 21 GDPR)
- Right to erasure (Art. 17 GDPR)
- Right to data portability (Art. 20)

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

International transfers

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

International transfers (i)

- **Basic principles remain the same**
  - Restrictions on transfers to non-adequate countries outside the EU
  - Existing adequacy decisions remain in force until amended, replaced or repealed
  - Authorizations granted by SAs and the existing Standard Contract Clauses (SCC) remain valid until amended, replaced or repealed
- **Major changes**
  - GDPR applies to onward transfers, irrespective of transfer mechanism used
  - Binding Corporate Rules (BCR) and SCC
    - BCR expressly recognized by the GDPR
    - no prior approval from SAs for transfers based on Commission SCC and approved BCR
    - local SAs authorized to issue own SCCs
  - Approved codes of conduct and seals
    - can now be used as a basis for international transfers

European Commission | ©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

International transfers (ii)

- **Major changes** (continued)
  - Derogations "for specific situations"
    - *consent*
      - must be explicit and transparent regarding the risks of the transfer
    - *compelling legitimate interest* introduced as a new derogation
      - subsidiary ground – only if contracts, BCRs or other derogations cannot be used
      - non-repetitive transfer
      - only for a limited number of data subjects
      - legitimate interest not overridden by the interests, rights, and freedoms of data subjects
      - controller assessed all the circumstances surrounding the transfer and applied suitable safeguards
      - obligation to inform the SA and the data subjects about the transfer

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Sanctions and enforcement

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Sanctions and enforcement

- **Fines**
  - Up to the greater of 2% of an undertaking's total annual worldwide turnover or €10 million for a large number of violations
  - Up to the greater of 4% of an undertaking's total annual worldwide turnover or €20 million for a more limited set of violations, including
    - *violation of data subject rights*
    - *violation of the basic principles for processing (legal basis, new consent rules, sensitive data)*
    - *violation of the data transfer rules*

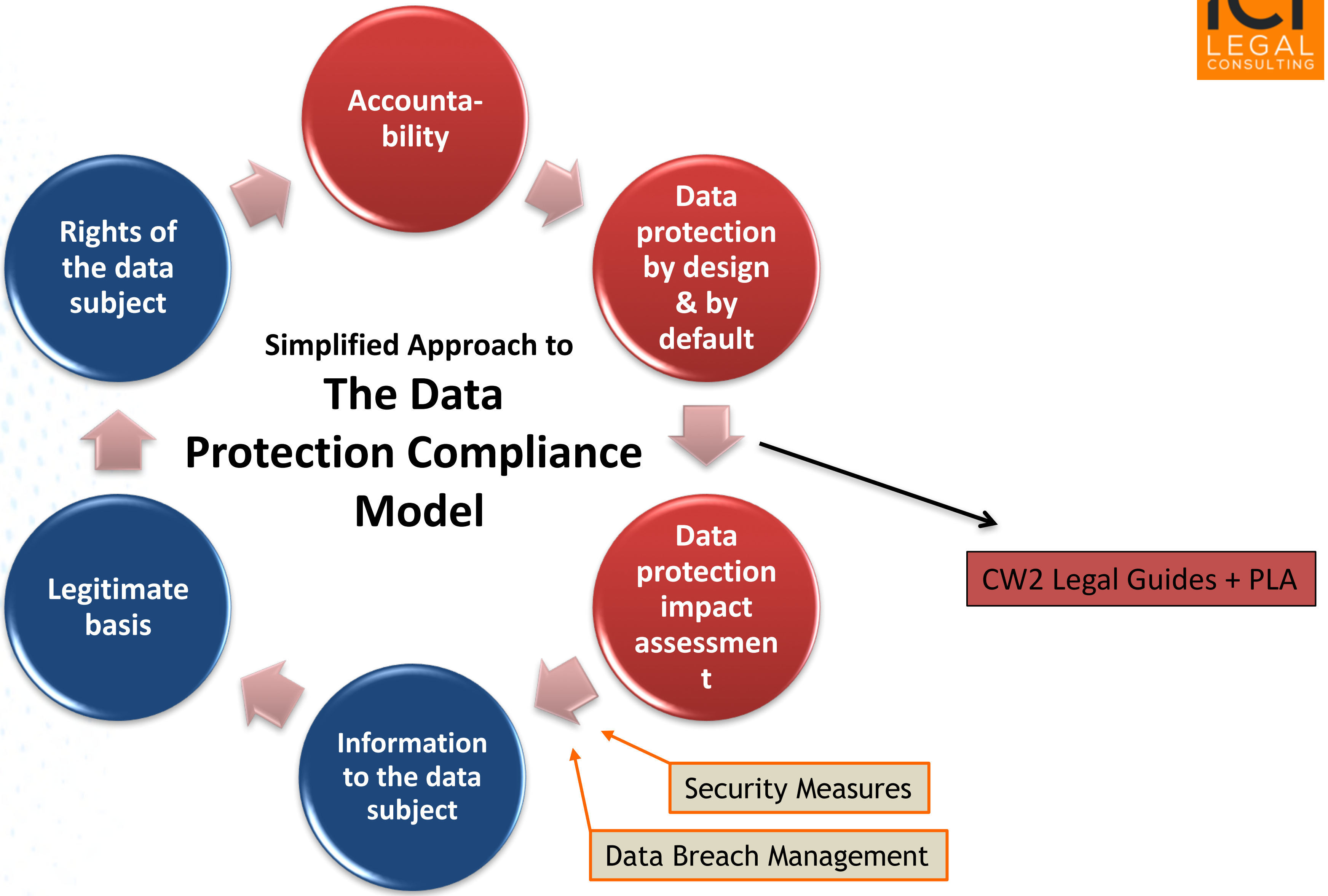
- **Data subjects' right to remedies**
  - Right to **lodge a complaint** with an SA for processing of their data in violation with the GDPR
  - Right to **start legal action**
  - - against an SA for failure to investigate a complaint or keeping the data subject informed
  - - against a controller or processor for processing of their data in violation with the GDPR (courts where controller or processor is established/courts of place of residence of data subject)
  - Right to **obtain compensation** for material or immaterial damage
  - - joint liability of controllers and processors for the entire damage
  - **Class actions**
  - - certain not-for-profit organizations can be mandated by data subjects to lodge complaints and claim compensation on their behalf
  - - Member States may also mandate organizations to act on behalf of data subjects

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

How to prepare

- ❑ **Review your governance structure**
- ❑ Review your privacy policies
- ❑ Prepare adequate data breach procedures and templates
- ❑ Prepare response mechanisms for data subject requests
- ❑ Start implementing privacy by design and by default
- ❑ Appoint a DPO
- ❑ Revise informed consent forms and methods to obtain consent
- ❑ Implement data protection impact assessments

European Commission | ©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748



©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Q&A (i)

- Many Equifax customers records that were compromised during the recent attack were of EU citizens (report at https://www.bloomberg.com/news/articles/2017-09-07/equifax-says-cyber-intrusion-affected-143-million-customers).
- Q. If this event at Equifax had occurred with GDPR post-enforcement (25 May 2018) what remedy would national regulators have against Equifax representing those citizens affected by the breach?
  - Equifax obligation to notify the SA;
  - Equifax obligation to notify users to the extent it is likely to result in a “high risk” for the rights and freedoms of individuals, subject to exceptions (*e.g.,* encryption)
  - SA to impose up to the greater of 2% of an undertaking’s total annual worldwide turnover or €10 million for a large number of violations
  - Data subjects’ right to claim compensation also through class actions

European Commission | ©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Q&A (ii)

- Are the US-headquartered cloud providers supporting EU regulations as diligently as the US equivalents. For example, AWS have quite sophisticated systems in place to help users manage HIPAA compliance. Are they doing the same for organisations managing Personally Identifiable Information for European Citizens?
  - Some of them yes i.e Tresorit (www.tresorit.com) and Rackspace (https://blog.rackspace.com/rackspace-launches-new-privacy-and-data-protection-offering) providing:
  - **Enhanced Data Protection** – Deploys technology platforms to restrict access to approved company personnel and processes, while generating detailed information about unauthorized access by users, applications and systems to sensitive data.
  - **Detailed Compliance Reporting** – Delivers detailed monthly reporting to provide customers with a comprehensive view of their data usage and how it is being protected, as well helps customers meet their compliance requirements in many regions including certain provisions in the European Union’s General Data Protection Regulation and PCI-DSS.

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Q&A (iii)

- What EU directives should a cloud provider consider when building out a channel sales strategy? Are there any restrictions on what vertical restraints that can be applied to channel partners?
  - **Mainly EU Antitrust law on vertical agreements listed at the following link: http://ec.europa.eu/competition/antitrust/legislation/vertical.html**

European Commission | ©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Q&A (iv)

- What are the legal risks, if any, for an individual working at a company, using a non-company, private email address for setting up an account with a cloud provider?
  - **Article 29 Working Party Opinion 2/2017 on data processing at work**
  - **ECHR case Bardulescu v. Romania:**
- provide a clear, prior **information notice** declaring the monitoring purposes;
- define the **legitimate legal grounds** allowing the monitoring;
- assess the **proportionality and subsidiarity** of the intended monitoring as defined in Article 29 Working Party Opinion 2/2017 in order see whether less intrusive means may achieve the same aim. This can form part of a Data Protection Impact Assessment (DPIA).

European Commission | ©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Q&A (v)

- Do cloud providers have to do anything along the lines of a “living will”, in order to ensure an orderly transfer of customers to another provider, in the event of a financial failure? There are various examples of particularly cloud storage providers like Nirvanix not doing this, resulting in problems with customers managing to migrate away
- Article 20 of the GDPR on the right to data portability.
- Proposal of Regulation on a framework for the free flow of non-personal data in the European Union

  Brussels, 13.9.2017 COM(2017) 495 final

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

Thank you for you attention!

©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

ICTLC I Senior Associate

Avv. NICOLA FRANCHETTO, LL.M. - Senior Associate

Nicola Franchetto is a qualified ICT, Privacy & Data Protection lawyer – Senior Associate at ICT Legal Consulting, Fellow of the European Privacy Association (Brussels) and the Italian Institute for Privacy (Rome).

He obtained an LL.M. (Master of Laws) in Information Technology and Intellectual Property at the Institute for Legal Informatics (IRI) (University of Hannover) (DE). Franchetto poses a very strong expertise on Data Security and Information Technology, effectively he operates in ICT Legal Consulting as *man in the middle* between the legal and the IT practical aspects related to personal data processing. Cloud computing, Big Data, Analytics and Internet of Things are areas in which he has developed significant experience.

GLOBAL LAW EXPERTS RECOMMENDED FIRM

The LEGAL 500 EMEA LEADING FIRM 2017

RECOMMENDED BY: FIVE STAR LAW ICT LAW | ITALY | 2015-2016

LEGALS FINEST RECOMMENDED LAW FIRM 2016

LEGALSFINEST 200

FIVE STAR LAW 2016 INFORMATION TECHNOLOGY TM

European Commission | ©2017 - CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748