Simmons & Simmons

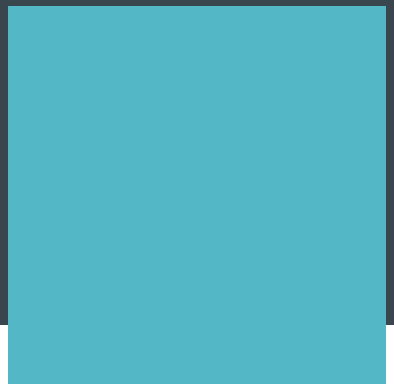
Simmons & Simmons Digital Day

Digitalisation & Cyber Security – a European Perspective

Alex Brown

Giorgio Mariani

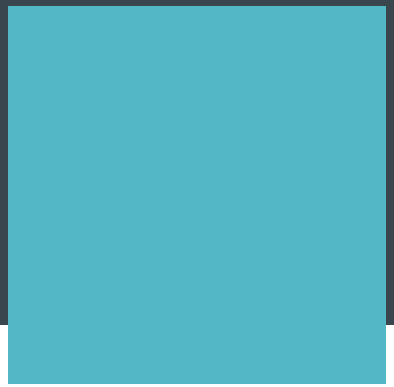
Christophe Fichet



Simmons & Simmons

UK
Digital Marketing & Cyber Security

Alex Brown



Simmons & Simmons

GDPR: Consequences for digital marketing

- Pro-active consent
  - Dealing with new customers
  - Preserving existing customer consents
- How granular does consent need to be?
- Is consent needed?
- Impact on profiling and personalisation – consent needed for profiling that produces a legal effect or has a significant impact
- E-Privacy Regulation
- Impact on data sharing arrangements and big data analytics

Cyber security – UK reflections

- 2017 UK Government survey:
  - 46% of businesses hacked
  - Most common type of breaches related to staff receiving fraudulent emails
  - Human factors involved in most breaches – staff awareness and training crucial
  - Protection of customer data seen as being the key driver for security expenditure

Cyber security – UK reflections

- Increased Governmental and regulatory focus
- NIS Directive or equivalent implementation in the UK?
- Increased focus on dealings with suppliers and other third parties
  - Contract provisions
  - Due diligence

Simmons & Simmons

Italy
M&A and Cybersecurity

Giorgio Mariani

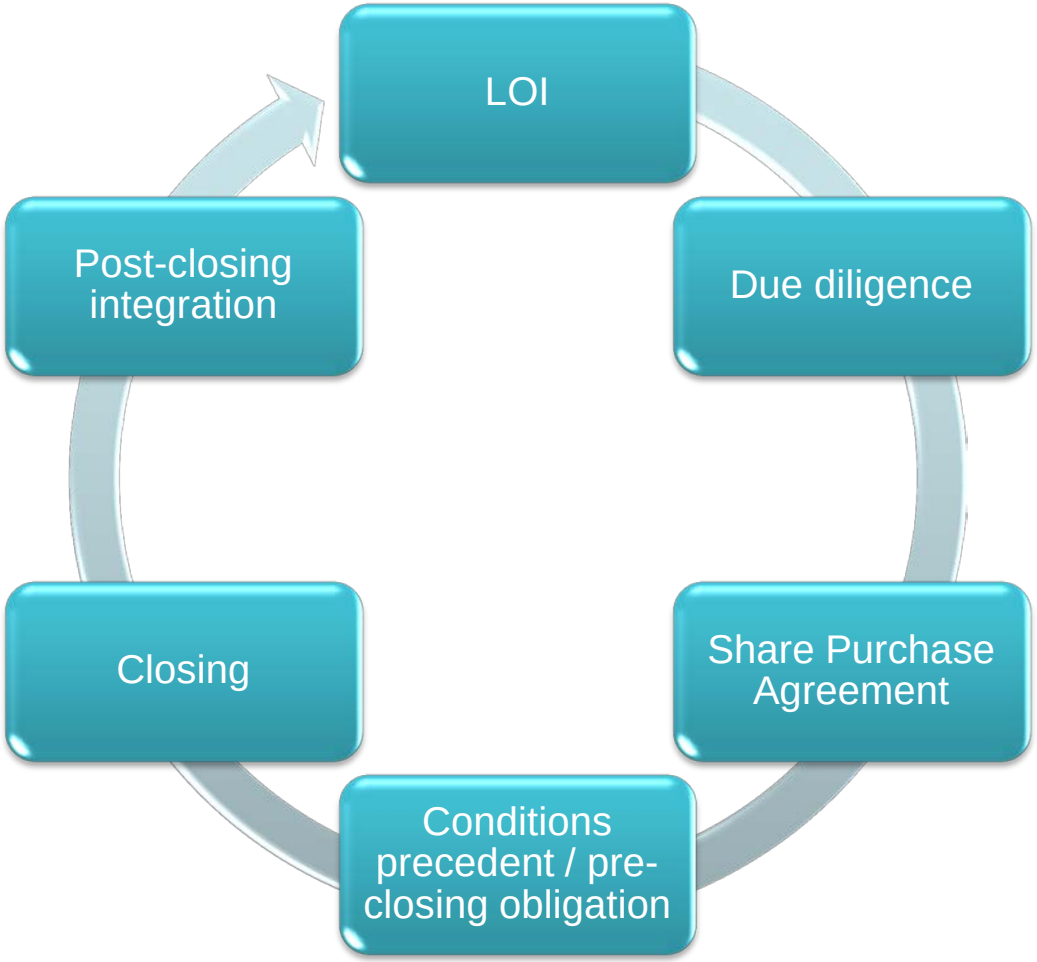
Cyberattacks: legal consequences

- IT systems incidents > NIS Directive
- Theft of personal data > GDPR
- Theft of IP/confidential information > breach of third party rights/agreements
- Business interruption > breach of contract
- Inside jobs > compliance issues

Would you buy a cyber-risk?

Simmons & Simmons

Quick recap of the M&A process



Simmons & Simmons

Cybersecurity and M&A

- Not considered a due diligence item
- Do M&A guys and IT guy talk?
- Cybersecurity and integration process

M&A process: due diligence

Simmons & Simmons

- Technical due diligence
- Legal due diligence
  - ✓ Cybersecurity policies > personnel
  - ✓ IT risk management
  - ✓ Incident response plan
  - ✓ Cyberattacks reports
  - ✓ Insurance policies (cyber-risks e business interruption)
  - ✓ Suppliers' due diligence / cyberwarranties

M&A process: pre-closing

- Interim period obligations of the seller > policies, disclosures, reports
- Condition precedent > cybersecurity audit
- MAE (*material adverse event*) clause > when the closing is far

M&A process: post-closing

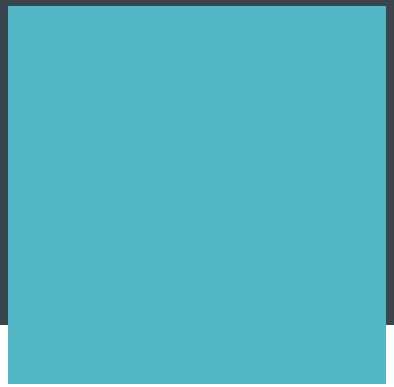
- R&W (*representations and warranties*) incidents, sanctions, thefts, etc.

- Indemnities

Simmons & Simmons

France
Digital regulatory update

Christophe Fitchet



Simmons & Simmons

Contents

1. Big data and data protection (1/3)

New decision of the *Conseil d'Etat* dated 8 February 2017

- **Background and CNIL's decision**

  On 16 July 2015, the French data protection authority (**CNIL**) **rejected** JCDecaux request for authorization of a processing of personal data for an experimentation of a **new analytics tool**.

  1. **Processing details**
     - WiFi mobile **tracking device** of pedestrians flow (via their mobile device) **located in La Defense** next to 6 of its billboards (25 meters radius)
     - **No consent** requested and **information of the individuals provided on the billboards (A4 paper)**
     - **But** alleged **almost immediate "anonymization"** of the personal data collected by cumulative methods of "**salting**" and "**key hashing**"
  2. **CNIL's legal grounds**
     - Legitimate interest: yes
     - **But**, the **methods used to anonymize the data were considered insufficient:**
       - JCDecaux was still in a position to identify the persons concerned
       - Purpose of the processing (tracking of pedestrians routes and passage repetition) was in contradiction with the concept of "anonymization"
       - and **thus**, the limited information for anonymized data (art. 32 IV of the law *Informatique et Libertés*) did not apply: full information was required and JCDecaux did not comply as the information JCDecaux had planned was insufficient

1. Big data and data protection (2/3)

New decision of the *Conseil d'Etat* dated 8 February 2017

- ***Conseil d'Etat*'s decision:**

  On 8 February 2017, the highest administrative court (*Conseil d'Etat* or **CE**) confirmed the CNIL's decision

  1. **Legal value of Article 29 WP's opinions: no normative value**
     - JCDecaux raised that the CNIL ignored Article 29 WP's Opinion 05/2014 on Anonymisation Techniques dated 10 April 2014: it recommended that the assessment of the risk of identification should be carried out in the light of the circumstances specific to each case
     - **Shift in legal analysis between Article 29 WP and national authority**
     - **Impact of GRDP**: may change this decision with the notion of supervisory authority and the obligation to cooperate with other national authorities involved in processing
  2. **Notion of anonymization: confirm CNIL's position on the lack of anonymization**
     - Data will not be considered anonymous when a unique identifier is associated to a data subject and the data controller is able to relate different data to that same identifier
     - Difficulties for IoT companies to rely on anonymization technique to provided only limited information
     - Additional costs associated with information notice and data subject rights' obligation as well as practicality issues
     - Potential negative impact on businesses using IoT and big data: it will be more difficult to avoid the data protection regulation (To be noted in GRDP: anonymised data fall out of the scope – no information requirements).

1. Big data and data protection (3/3)

New decision of the *Conseil d'Etat* dated 8 February 2017

- ***Conseil d'Etat*'s decision:**
  - **3. Notion of "indirect" collection**
    - No intervention of the individual concerned in the processing
    - JCDecaux tried to argue that the processing was an "indirect" collection
      - This could trigger an exception to the information obligation when "the provision of such information proves impossible or would involve a disproportionate effort" (Art. 32-III of French data protection law)
    - Nevertheless, the CE decided that it was a "direct" collection of personal data – **no exception possible**
    - Therefore, the use of such technical sensor is not considered as an indirect collection
    - Difficulties for IoT in terms of increased costs and practicality issues
    - CE's decision is even more impacting as the GDPR provides for this same exception (Art.14 5. b) GDPR).

2. Blockchain in French securities law (1/2)

- ***Minibons* (type of securities) can be represented and transmitted using distributed ledger technology (DLT):**
  1. **Law**: Law No. 2015-990 of 6 August 2015 for growth, activity and equality and equal economic opportunity (Article 168)
     - grants the Government power (within 9 months) to reform securities laws on *minibons*
  2. **Ordinance**: Ordinance No. 2016-520 of 28 April 2016 on *minibons*
     - **Issuance**:
       - Securities issued via **internet crowdfunding platforms**
       - **Platforms** having the status of *Conseil en investissement participatif* (**CIPs**) or *Prestaire de services d'investissement* (**PSIs**); (Art. L.223-6 of the Monetary and Financial Code)
       - Same rules of conduct applicable to CIPs and PSIs for the intermediation of shares and bonds and *minibons* (e.g. competence, declaration, transparency, test of the suitability of the offer to the investor's profile…)
     - **Suscription**: suscription possible by natural or legal persons
     - **Transfer of ownership**:
       - Transfer of *minibons* may be handled via DLT using **blockchain** (Article L.223-12)
       - Transfer qualifies as a **written contract** (Article L.223-13).
  3. **Decree**: A **decree specifying the conditions of issue and transfer of *minibons* using blockchain is still awaited**

2. Blockchain in French securities law (2/2)

- **Extension to all securities**
  1. **Law**: Article 120 of Law No. 2016-1691 of the Transparency, Anti-Corruption and Economic Modernisation Act dated 9 December 2016 « **Loi Sapin II** »
     - grants the Government power (up until 9 December 2017) to reform securities laws
     - so that securities that are not traded via a central securities depository and a securities settlement system can be represented and transmitted using distributed ledger technology (DLT)
  2. **Ordinance**: Ongoing public consultation from the *Trésor* on the scope of the required reform of security law (response required before 19 May 2017)
- **Impacts:**
  - Recognition of the legal value of blockchain paves the way for more applications of this technology in the future
  - Government's will to diversify the means for financing companies via alternative credit channels
  - Possible challenge to banking monopoly on credit (comparable trend concerning payment methods)
  - BNP Paribas Securities Services and crowdfunding platform SmartAngels have already announced a partnership on minibons based on blockchain

Simmons & Simmons

simmons-simmons.com
elexica.com